#2

Attorney Docket No. 1341.1108

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Satoru TORII, et al.

Application No.: Group Art Unit:

Filed: September 20, 2001 Examiner:

For: METHOD OF AND SYSTEM FOR MANAGING INFORMATION, AND COMPUTER PRODUCT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-387880

Filed: December 20, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 20, 2001 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年１２月２０日

出願番号
Application Number: 特願２０００－３８７８８０

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　６月　４日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０５２４９３

【書類名】　特許願

【整理番号】　0051969

【提出日】　平成12年12月20日

【あて先】　特許庁長官殿

【国際特許分類】　H04K　3/00

【発明の名称】　情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　鳥居　悟

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　三友　仁史

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　滝沢　文恵

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100089118

【弁理士】

【氏名又は名称】　酒井　宏明

【手数料の表示】

【予納台帳番号】　036711

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9717671

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項１】　通信要求を監視する通信要求監視手段と、前記通信要求監視手段から通知された情報に基づいて対策を選択する管理手段と、前記管理手段からの指示に応答して対策を実施する実施手段とを有し、

前記管理手段は、

前記通信要求監視手段からの通知内容と前記実施手段が実施する対策とを対応づけて管理するデータベースと、

前記データベースに基づいて対策を選択する選択手段と、

を備えたことを特徴とする情報管理システム。

【請求項２】　攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集手段と、前記情報収集手段により収集整理された情報を前記データベースに反映する反映手段と、をさらに備えたことを特徴とする請求項１に記載の情報管理システム。

【請求項３】　前記選択手段は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする請求項１または２に記載の情報管理システム。

【請求項４】　前記データベースは、前記通信要求監視手段により通知される情報を時系列で保持し、前記選択手段は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする請求項１、２または３に記載の情報管理システム。

【請求項５】　前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成手段をさらに備えたことを特徴とする請求項１～４のいずれか一つに記載の情報管理システム。

【請求項６】　システムの脆弱性を示す脆弱性呈示手段と、前記脆弱性呈示手段に対する攻撃に関する情報を収集する情報収集手段と、をさらに備えたこと

を特徴とする請求項１～５のいずれか一つに記載の情報管理システム。

【請求項７】　通信内容の発信元を調査する調査手段と、前記調査手段による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定手段と、をさらに備えたことを特徴とする請求項１～６のいずれか一つに記載の情報管理システム。

【請求項８】　攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに備えたことを特徴とする請求項１～７のいずれか一つに記載の情報管理システム。

【請求項９】　通信要求を監視部によって監視する通信要求監視工程と、

前記通信要求監視工程により通知される通知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、

前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、

を含んだことを特徴とする情報管理方法。

【請求項１０】　通信要求を監視部によって監視する通信要求監視工程と、

前記通信要求監視工程により通知される通知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、

前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、

をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる情報管理システム、情報管理方法および記録媒体に関する。

【０００２】

【従来の技術】

近年のネットワーク技術の進展に伴って、インターネット上の分散システムであるＷＷＷ（World Wide Web）の利用が急速に拡大し、情報を提供する各種ＨＴ

ＴＰサーバも累増してきたが、かかるサーバの増加とともに不正アクセスも増加しつつある。

【０００３】

この不正アクセスには、ネットワーク上のセキュリティホールを探知し、このセキュリティホールを介してシステムに侵入攻撃するものが知られており、この場合には、（１）稼働ホストを探知し、（２）提供サービスを探知し、（３）ネットワーク構成を探知し、（４）ＯＳを識別し、（５）アプリケーションを識別し、（６）セキュリティホールを探知するという手順でセキュリティホールが探知される。そして、複数の踏み台サイトを使用してターゲットに対して大量のパケットを送り込むなどしてシステムエラーを導き、その後不正アクセスがなされることになる。

【０００４】

ここで、この不正アクセスは、一般的なアクセスと明確に区別することができないため、通常は進入攻撃がおこなわれるまでシステム管理者が不正アクセスを検知することが難しいという特性がある。

【０００５】

このため、従来は、サイトに対して送り込まれる大量のパケットを認識した際に、できる限り迅速に不正アクセスによる実被害を極小化する対策が採られるのが一般的である。

【０００６】

【発明が解決しようとする課題】

しかしながら、ターゲットとなるサイトに一旦攻撃が開始されると、この攻撃を防御することは極めて難しく、また理想的な対策を講じたとしても、一時的にサイトを閉鎖せざるを得ないという問題が生ずる。特に、銀行や交通機関のように多数のユーザに対して継続的にサービスを提供するサイトでは、一時的にサイトを閉鎖することによる影響が各方面に波及し、膨大な実被害をもたらす可能性もある。

【０００７】

このため、かかる不正アクセスによる被害をいかに極小化するかが極めて重要

な課題となっており、望ましくは、不正アクセスがなされたとしても全く被害が生じない枠組みが必要とされている。

【０００８】

この発明は、上述した従来技術による課題を解消するためになされたものであり、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【０００９】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項１、９および１０の発明によれば、図２に示すデータベース２０１内に通知内容（Ａ）と対策（Ｂ）を対応づけて保持しておき、モニタエージェント２０３（通信要求監視手段）が通信要求を監視して異常を検知して管理マネージャ２０２（管理手段）に通知すると、この管理マネージャ２０２（管理手段）が、データベース２０１から対策を選択して、アクションエージェント２０４（実施手段）に対策を実行させることとしたので、対策を効率良く実行することができ、もって、実際の攻撃に適切な対策を施して被害の極小化を図ることができる。

【００１０】

また、請求項２の発明によれば、攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベースに反映することとしたので、データベースの内容を充実させ、より適切な対策を選択することができる。

【００１１】

また、請求項３の発明によれば、データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することとしたので、データベースのみならずシステムを取り巻く環境を考慮した上で妥当な対策を選択することができる。

【００１２】

また、請求項４の発明によれば、データベースが通信要求監視手段により通知される情報を時系列で保持し、このデータベースに記憶した時系列の情報に基づいて対策を選択することとしたので、時系列的な情報を用いて対策を選択することができる。

【００１３】

また、請求項５の発明によれば、複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成することとしたので、空間的な情報を用いて対策を選択することができる。

【００１４】

また、請求項６の発明によれば、システムの脆弱性を明示的に呈示し、この脆弱箇所に対する攻撃に関する情報を収集することとしたので、悪意者による攻撃手法を把握することができる。

【００１５】

また、請求項７の発明によれば、通信内容の発信元を調査した調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定することとしたので、踏み台とされているサイトを効率良く特定することができる。

【００１６】

また、請求項８の発明によれば、攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、この攻撃対象サイトへの攻撃を回避させるおとりサイトを設けることとしたので、攻撃対象サイトの保全を図るとともに攻撃手法を把握することができる。

【００１７】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係る情報管理システム、情報管理方法、およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００１８】

まず、本実施の形態に係る全体システムに採用した各種技術について説明する。図１は、本実施の形態に係る全体システムに採用した各種技術を説明するため

の説明図である。同図に示すように、このシステムでは、誘導／情報収集技術、データベース化技術、予知技術、信頼性回避技術および攻撃回避技術などを駆使している。

【００１９】

具体的には、この誘導／情報収集技術は、脆弱性を表に出して攻撃者（悪玉ハッカー）１０１による攻撃をおとりサーバ１０２に誘導するものであり、アンダーグラウンド情報、被害サイト情報並びに誘導して起こした攻撃によって攻撃に関する情報を収集し、得られた情報を解析して攻撃パターンとして認識する。

【００２０】

また、データベース化技術は、解析した攻撃パターン、被害予想、対策案をデータベース化するものであり、たとえば、図中に示したＵＧ系サイト群（善玉ハッカー）１０３、おとりサーバ１０２および被害サーバ１０４に対するアクセス手法とその対策を事例データベース１０５に蓄積する。

【００２１】

また、予知技術は、事例データベース１０５を用いて、現時点で起こっている状況から攻撃の予兆を検知し、これにより起こり得る攻撃を予知するものであり、具体的には、攻撃者１０１による現時点での状況をパケットモニタ群１０６で検知する。

【００２２】

また、攻撃回避技術は、事例データベース１０５を用いて、攻撃の進捗、環境などの情報から現時点で最適な回避対策を選択するものであり、たとえば図中の踏み台群１０７を踏み台とする防御対象サーバ１０８への攻撃をおとりサーバ１０９に誘導して攻撃を回避する。また、信頼性検知技術は、攻撃元と思われるサイトに対して、たとえば踏み台になっていないかなどの検査をおこなうものである。

【００２３】

次に、図１に示した予知技術についてさらに詳細に説明する。この予知技術は、現実の攻撃あるいは誘導して起こした攻撃において、そのパターンの解析から、単発だけではなく、複数の種々の事象を空間的／時間的に連携づけた形で攻撃

を起こす予兆をデータベース化し、その予兆に対する攻撃の影響範囲、影響度合い、被害レベルを関連づけた形で整備し、半自動的にアップデートする。

【００２４】

また、単発だけではなく、複数の種々の事象を関連づけた形で認識し、事例データベース１０５に照らし合わせて、予兆あるいは予兆候補として検知する。そして、検知した予兆および予兆候補を自ら解釈するだけではなく、下流サイトなどの他サイトへ通知する。

【００２５】

さらに、自ら検知したサイトまたはたとえば上流サイトから通知された予兆および予兆候補から、事例データベース１０５に照らし合わせて、将来起こり得る攻撃を予知する。この攻撃の予知は、事例データベース１０５の情報にしたがって、影響範囲、影響度合い、被害レベルなどについておこなう。

【００２６】

このように、かかる予知技術は、（１）不正アクセス手法とその予兆現象のデータベース化、（２）予兆検知、（３）予兆／予兆候補通知、（４）攻撃予兆などからなる。

【００２７】

（１）不正アクセス手法とその予兆現象のデータベース化

アンダーグラウンド（ＵＧ）系サイト群１０３で公開される不正アクセス手法を収集および解析し、被害サーバ１０４（他サイト）で実際に発生した攻撃手法を収集および解析し、おとりサーバ１０２によって脆弱性を表に出して攻撃を誘導し、その攻撃手法を収集および解析する。

【００２８】

そして、これらの解析結果をもとに、単発だけではなく複数の種々の事象を空間的／時間的に連携づけた形で攻撃パターンの解析をおこない、攻撃を起こす予兆をデータベース化する。その予兆に対する攻撃の影響範囲、影響度合い、被害レベルを関連づけた形で整備し、事例データベース１０５を半自動的にアップデートする。

【００２９】

（２）予兆検知

特定サイトへ向けた定常状態とは異なるパケット到着状態を検出し、また特定サイトでの定常状態と異なるパケット到着状態を検出し、これらの検出結果をもとに、単発だけではなく複数の種々の事象を連携づけた形で認識し、この認識結果をもとに、事例データベース１０５の内容と照らし合わせて、予兆または予兆候補を検知する。

【００３０】

（３）予兆／予兆候補通知

検出した予兆および予兆候補をたとえば下流サイトのような他サイトに通知する。たとえば、特定サイトへ向けた定常状態とは異なるパケット発信を依頼された際には、そのパケットを送信するとともに、「このパケットは○○攻撃の予兆である可能性がある」という情報を、そのサイトに通知する。

【００３１】

（４）攻撃予兆

自ら検知し、また上流サイトのような他サイトから通知された予兆および予兆候補を事例データベース１０５の内容と照らし合わせることにより、将来起こり得る攻撃を予知する。

【００３２】

次に、図１に示した攻撃回避技術についてさらに詳細に説明する。この攻撃回避技術は、攻撃を受けた履歴から、攻撃の進捗過程のそれぞれにおける回避手段を攻撃対象の種別、環境条件ごとに考察し、その回避手段を、予兆／攻撃と関連づける形でデータベース化し、半自動的にアップデートする。

【００３３】

そして、攻撃を予知した後に、現時点が予知された攻撃のどの段階にあるのかを予測し、攻撃対象、環境条件を見いだし、事例データベース１０５から最適の回避手段を決定する。その後、決定した回避手段を行使して、攻撃を未然に防止する。したがって、かかる攻撃回避技術は、（１）回避手段のデータベース化、（２）回避手段の選択、（３）回避手段の行使などからなる。

【００３４】

（１）回避手段のデータベース化

攻撃を受けた履歴から、攻撃の進捗過程のそれぞれにおける回避手段を、攻撃対象の種別、環境条件ごとに考察、開発および検証し、その回避手段を予兆／攻撃と関連づける形でデータベース化し、半自動的にアップデートする。

【００３５】

（２）回避手段の選択

攻撃を予知した後、現時点が予知された攻撃のどの段階にあるかを予測する。そして、予知した攻撃の対象を見極め、環境条件を見いだす。そして、攻撃の進捗具合、攻撃対象、環境条件を事例データベース１０５と照らし合わせて最適の回避手段を決定する。

【００３６】

（３）回避手段の行使

攻撃を予知する材料となった予兆／予兆候補を通知した上流サイトに対して通知し、その予兆／予兆候補のもととなったパケット発信元の信頼性検査を促す。また、攻撃の被害の拡大を防ぐため、破棄すべきパケットを選定してこれを破棄する。さらに、攻撃の被害の拡大を防ぐため、破棄すべきパケットを選定し、そのパケットを発信する可能性がある上流サイトに対して発信をしないように促す。また、攻撃を受けつつあることを他のサイトに通知して、同様の攻撃が他のサイトにおこなわれないよう促す。さらに、攻撃を検知したサイトを模したおとりサーバ１０９を設け、それ以降の攻撃をおとりサーバ１０９側へと導く。

【００３７】

ここで、このおとりサーバ１０２および１０９について具体的に説明する。かかるおとりサーバ１０２および１０９は、脆弱性があるふりをして攻撃を誘うサーバであり、（１）ユーザ名の変更（管理者権限）、（２）ログインメッセージ（ＯＳや版数）の変更、（３）アプリケーション名や版数の変更、（４）稼働ネットワークの偽称、（５）脆弱なＣＧＩプログラムの存在を偽称などを通じて、脆弱性があるふりをする。

【００３８】

（１）ユーザ名の変更（管理者権限）

たとえば、ウインドウズにおいて、初期設定時には管理者権限を持つユーザは「Administrator」であるが、新規にユーザ「Kanrisya」を設定して管理者権限を持たせ、従来のユーザ「Administrator」から管理者権限を外すことにより、システムが脆弱であるかの如く思わせることができる。

【００３９】

（２）ログインメッセージ（ＯＳや版数）の変更

通常のSolarisマシンにおけるログインメッセージは、下記のようになる。

```
SunOS 5.6
login:user-name
Password:********
last login: Tue Aug 29 08:52:55 on console
Sun Microsystems Inc.  SunOS 5.6    Generic August 1997
%
```

【００４０】

ここで、以下のように表示するようにログインメッセージを変更し、現実とは別の（古いシステムで過去の脆弱性が残っている）ＯＳが稼働しているように見せることにより、システムが脆弱であるかの如く思わせることができる。

```
TurboLinax release 3.2(***)
Kernel 1.2.9 on an i386(host.domain.company.co.jp)
login:user-name
Password:********
%
```

【００４１】

（３）アプリケーション名や版数の変更

ウエブサーバに対して、HEADメッセージを送付すると、以下のようにサーバアプリケーション名を返す。

```
HTTP/1.1 200 OK
Data:Sat,1 Jan 2000 10:25:12 GMT
Server:Apache/1.3.9(Unix)
```

【００４２】

ここで、以下のように返答メッセージを変更し、現実とは別のアプリケーション（古いシステムで過去の脆弱性が残っているもの）が稼働しているように見せることにより、システムが脆弱であるかの如く思わせることができる。

```
HTTP/1.0 200 OK
Server:Microsoft-IIS/3.0
Date:Sat,01 Jan 2000 10:25:25 GMT
```

【００４３】

（４）稼働ネットワークの偽称

ポートスキャンなどの悪用ツールを用いることで、稼働中のネットワークサービスを調査することができる。

Port	State	Protocol	Service
21	open	tcp	ftp
80	open	tcp	www-http
443	open	tcp	https

【００４４】

ここで、虚偽の「ネットワークサービス受付機構」を用意し、その虚偽サービス（脆弱なサービス，port 23,79,110,111,143）へのアクセスをすべて監視するようにする。その結果として、ポートスキャンなどの悪用ツールにより、以下のような（虚偽の）調査結果が得られ、脆弱なサービスが稼働しているように誤認させることができる。

Port	State	Protocol	Service
21	open	tcp	ftp
23	open	tcp	telnet
79	open	tcp	finger
80	open	tcp	www-http
110	open	tcp	pop3
111	open	tcp	sunrpc
143	open	tcp	imap

443　open　tcp　https

【００４５】

（５）脆弱なＣＧＩプログラムの存在を偽称

スキャンツールなどの悪用ツールを用いることで、提供可能なＣＧＩプログラムの存在が検査できる。

```
Searching for _vti_inf.html　:[Not Found]
Searching for service.pwd　:[Not Found]
Searching for users.pwd　:[Not Found]
Searching for authors.pwd　:[Not Found]
Searching for administrators　:[Not Found]
Searching for shtml.dll　:[Not Found]
Searching for shtml.exe　:[Not Found]
...
Searching for [perl.exe ].　:[Not Found]
Searching for [wwwboared.pl]　:[Not Found]
Searching for [www-sql].　:[Not Found]
```

【００４６】

ここで、脆弱性の存在が知られている既知のＣＧＩプログラム（と同一名のファイル）を用意しておく。

```
% touch cgi-bin/phf cgi-bin/Count cgi-bin/test-cgi cgi-bin/phf.cgi
% touch cgi-bin/webgais cgi-bin/perl.exe cgi-bin/www-sql
% touch _vti_inf.html
% mkdir _vti_bin _inf.html _vti_pvt cfdocs
% touch _vti_bin/shtml.exe _vti_pvt/service.pwd _vti_pvt/authors.pwd
% touch cfdocs/zero.cfm cfdos/root.cfm
```

【００４７】

結果として、スキャンツールなどの悪用ツールにより、以下のような（虚偽の）調査結果が得られ、脆弱なＣＧＩプログラムが存在しているように認識させることができる。

```
Searching for _vti_inf.html        :[Found!]
Searching for service.pwd          :[Found!]
Searching for users.pwd            :[Not Found]
Searching for authors.pwd          :[Found!]
Searching for administrators       :[Not Found]
Searching for shtml.dll            :[Not Found]
Searching for shtml.exe            :[Found!]
...
Searching for [perl.exe ].         :[Found!]
Searching for [wwwboared.pl]       :[Not Found]
Searching for [www-sql].           :[Found!]
```

【００４８】

次に、本実施の形態に係る情報管理システムの基本構成などについて図２～図１３を用いて説明する。図２は、本実施の形態に係る情報管理システムの基本構成を示すブロック図である。同図に示すように、この情報管理システムは、データベース（ＤＢ）２０１を有する管理マネージャ２０２と、モニタエージェント２０３と、アクションエージェント２０４とからなる。

【００４９】

このデータベース２０１には、データＡと対策Ｂが対応づけて蓄積されており、管理マネージャ２０２は、モニタエージェント２０３からデータＡの通知を受け付けたならば、データベース２０１の内容を参照して対策Ｂおよび対策の依頼先（アクションエージェント２０４）を特定し、このアクションエージェント２０４に対して対策Ｂの実行を指示する。また、攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベース２０１に反映する。

【００５０】

具体的には、モニタエージェント２０３が、ファイアウオールやWWWサーバ（以下、「エンティティ」と言う）のログを分析して異常を検知したならば、異常が発生した旨を示すデータＡを管理マネージャ２０２に通知する。そして、管

理マネージャ２０２は、データベース２０１を参照して対策Ｂを特定する。具体的には、このデータベース２０１は、モニタエージェント２０３から通知されたデータを時系列で保持し、この時系列のデータに基づいて管理マネージャ２０２が対策Ｂを選択する。

【００５１】

たとえば、この対策Ｂとしては、「WWWサーバに異常が発生した場合に、ファイアウオールやWWWサーバへの通信を通さないようにする」という対策などがある。なお、図３に示すように、かかるモニタエージェント２０３およびアクションエージェント２０４は、複数存在しても良い。

【００５２】

ここで、上記モニタエージェント２０３は、データＡを取得した際に該データＡそのものを管理マネージャ２０２に通知することとしたが、図４に示すように、管理マネージャ２０２が、重み付けしたデータＡと重み付けした対策Ｂを対応づけて保持することもできる。

【００５３】

図５は、かかる場合におけるモニタエージェント２０３の構成を示すブロック図である。同図に示すように、モニタエージェント２０３は、データ解析部２０３ａ、データ分析部２０３ｂ、データスタック２０３ｃ、重みテーブル２０３ｄ、判定処理部２０３ｅおよび通知部２０３ｆからなる。

【００５４】

すなわち、このモニタエージェント２０３は、データ解析部２０３ａによりデータＡをデータ解析し、データ分析部２０３ｂによりそのデータを分析して、データスタック２０３ｃに蓄積する。このデータスタック２０３ｃに蓄積されるデータは、時系列ごとに保持される。そして、あらかじめ準備した重みテーブル２０３ｄに基づいて、判定処理部２０３ｅが重みを判定し、通知部２０３ｆが重み付きの事象Ａを管理マネージャ２０２に通知する。なお、かかる重み付けに用いる重み係数は、ユーザが任意に設定することができ、また、実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定することもできる。

【００５５】

次に、図２に示した管理マネージャ２０２について説明する。図６は、図２に示した管理マネージャ２０２を説明するための説明図である。同図に示すように、この管理マネージャ２０２は、すでに説明したように、モニタエージェント２０３からデータＡを受け付けた際に、データベース２０１を参照して対策Ｂを特定することになるが、この際、システム構成２０５および運用状況２０６などについても考慮する。

【００５６】

また、この管理マネージャ２０２では、図７に示すように、各モジュール２０７からサイトに関する空間情報を取得し、取得した空間情報に基づいてサイトの物理マップ（サイトマップ）２０８を作成する。なお、ここで言うモジュール２０７には、各種モニタエージェント２０３およびアクションエージェント２０４が含まれる。

【００５７】

また、図８に示すように、この管理マネージャ２０２は、モニタエージェント２０３に対してフィードバックをおこなっており、具体的には、管理マネージャ２０２は、モニタエージェント２０３のデータ分析部２０３ｂで使用する分析ルールをモニタエージェント２０３に対して配布する。このように、管理マネージャ２０２の主導のもとに、モニタエージェント２０３の分析ルールが更新される。このため、上記サイトマップ２０８に基づいて、監視対象となる通信の種類および／または時間を各モニタエージェント２０３に配布されることになる。

【００５８】

次に、モジュール間の相互情報参照について説明する。図９は、モジュール間の相互情報参照を説明するための説明図である。なお、ここでは説明の便宜上、それぞれ２台の管理マネージャー、モニタエージェントおよびアクションエージェントを設けた場合を示している。

【００５９】

すでに説明したように、モニタエージェント２０３から管理マネージャ２０２へデータＡが送信されると、この管理マネージャ２０２からアクションエージェント２０４に対して対策Ｂが指示されるわけであるが、モニタエージェント２０

３～モニタエージェント２０３’、アクションエージェント２０４～アクションエージェント２０４’、管理マネージャ２０２～管理マネージャ２０２’の間でも情報の相互参照がおこなわれる。

【００６０】

次に、図２に示したデータベース２０１の自動更新について説明する。図１０は、図２に示したデータベース２０１の自動更新（ＰＵＬＬ型）を説明するための説明図である。同図に示すように、データベース２０１を更新する管理データベース２０２では、コレクタ部１００１がセレクションデータ１００２に基づいて、ネットワーク１００３に所在するサイトに対してリクエストを発してデータを収集する。具体的には、タイマ１００４がタイムアウトした時点で、コレクタ部１００１がセレクションデータ１００２を読み込み、このセレクションデータ１００２に対応するデータをリクエストする。

【００６１】

そして、このコレクタ部１００１が各サイトから取得したデータをフォーマッタ１００５に出力してフォーマット変換などをおこない、その結果をライタ１００６がデータベース２０１に書き込む。

【００６２】

ところで、かかるデータベース２０１の自動更新は必ずしもＰＵＬＬ型でおこなう必要はなく、図１１に示すようにＰＵＳＨ型でおこなうこともできる。かかるＰＵＳＨ型でデータベース２０１を自動更新することとすると、ネットワークに存在するサイトからデータベース２０１に自動的にデータが送り込むことができ、かつ、管理マネージャ２０２の構成が簡素化することができる。

【００６３】

また、図１２に示すように、ＰＵＳＨ型システムの管理マネージャ２０２内にユーザインターフェース１００７を設けると、ユーザの発意のもとに所望のサイトに対してリクエストを発することができる。さらに、図１３に示すように、ＰＵＬＬ型システムの管理マネージャ２０２内にユーザインターフェース１００７を設けると、ネットワークに存在するサイトから自動的に送り込まれたデータをユーザの発意に基づいてデータベース２０１内に取り込むことができる。

【００６４】

次に、図２に示した管理マネージャ２０２、モニタエージェント２０３およびアクションエージェント２０４による処理手順について説明する。まず、モニタエージェント２０３が異常を検知してからアクションエージェント２０４が対策を実施するまでの処理手順について説明する。

【００６５】

図１４は、モニタエージェント２０３が異常を検知してからアクションエージェント２０４が対策を実施するまでの処理手順を示すフローチャートである。同図に示すように、モニタエージェント２０４は、エンティティのログを分析して（ステップＳ１４０１）、異常の有無を確認する。その結果、異常を検知した場合には（ステップＳ１４０２肯定）、管理マネージャ２０２に対して異常を通知する（ステップＳ１４０３）。

【００６６】

そして、管理マネージャ２０２は、データベース２０１などを参照して対策および対策依頼先を決定し（ステップＳ１４０４）、対策依頼先であるアクションエージェント２０４に対して対策を依頼する（ステップＳ１４０５）。

【００６７】

この対策の依頼を受けたアクションエージェント２０４は、指示された対策を実施し（ステップＳ１４０６）、対策結果を管理マネージャ２０２に対して通知する（ステップＳ１４０７）。この対策結果を受け取った管理マネージャ２０２は、対策結果をディスプレイに表示するなどしてユーザに報告する（ステップＳ１４０８）。

【００６８】

ところで、ユーザは、エンティティを対策実施前の状態に戻すことを望む場合が多いので、本実施の形態では、かかるエンティティの対策復元も可能としている。図１５は、エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャートである。

【００６９】

同図に示すように、ユーザが管理マネージャ２０２のメニューから「対策復元

」を選択し（ステップＳ１５０１）、対策を復元するエンティティを指定すると（ステップＳ１５０２）、管理マネージャ２０２は、指定されたエンティティの対策履歴を表示する（ステップＳ１５０３）。

【００７０】

ここで、ユーザが対策履歴から復元する対策を選択すると（ステップＳ１５０４）、管理マネージャ２０２は、対策依頼先となるアクションエージェント２０４に対策を依頼する（ステップＳ１５０５）。

【００７１】

そして、このアクションエージェント２０４は、依頼された対策を実施して（ステップＳ１５０６）、対策結果を管理マネージャ２０２に通知し（ステップＳ１５０７）、管理マネージャ２０２は、この対策結果をユーザに報告する（ステップＳ１５０８）。

【００７２】

次に、図２に示した管理マネージャ２０２における対策ルールの更新手順について説明する。図１６は、図２に示した管理マネージャ２０２における対策ルールの更新手順を説明するための説明図である。同図に示すように、ユーザは、入手した対策ルールを適当な（所定の）ディレクトリに置き（ステップＳ１６０１）、管理マネージャ２０２のメニューから「対策ルール更新」を選択する（ステップＳ１６０２）。

【００７３】

そして、ユーザが、新しい対策ルールのファイルパス名を指定したならば（ステップＳ１６０３）、管理マネージャ２０２は、オブジェクトの属性、対策ルールファイル名を更新する（ステップＳ１６０４）。

【００７４】

次に、図２に示した管理マネージャ２０２において対策プランをカスタマイズする際の処理手順について説明する。図１７は、図２に示した管理マネージャ２０２において対策プランをカスタマイズする際の処理手順を示すフローチャートである。

【００７５】

同図に示すように、ユーザが、管理マネージャ２０２のメニューから「対策プランカスタマイズ」を選択すると（ステップＳ１７０１）、管理マネージャ２０２は、対策プランを編集する対策プランエディタを起動する（ステップＳ１７０２）。

【００７６】

そして、この対策プランエディタが起動したならば、ユーザは、このエディタを用いて対策プランをカスタマイズし（ステップＳ１７０３）、管理マネージャ２０２は、オブジェクトの属性、対策プランファイル名を更新する（ステップＳ１７０４）。

【００７７】

次に、分析ルールを更新する際の管理マネージャ２０２とモニタエージェント２０３の処理手順について説明する。図１８は、分析ルールを更新する際の管理マネージャ２０２とモニタエージェント２０３の処理手順を示すフローチャートである。

【００７８】

同図に示すように、ユーザが入手した分析ルールを適当なディレクトリに置き（ステップＳ１８０１）、管理マネージャ２０２のメニューから「分析ルール更新」を選択し（ステップＳ１８０２）、新しい分析ルールのファイルパス名と、分析ルールを送るモニタエージェント２０３を指定すると（ステップＳ１８０３）、管理マネージャ２０２は、この分析ルールをモニタエージェント２０３に配布する（ステップＳ１８０４）。

【００７９】

その後、このモニタエージェント２０３は、分析ルール更新し（ステップＳ１８０５）、管理マネージャ２０２に対して更新結果を返し（ステップＳ１８０６）、管理マネージャ２０２は更新結果をユーザに報告する（ステップＳ１８０７）。

【００８０】

次に、分析ルールをカスタマイズする際の管理マネージャ２０２とモニタエージェント２０３の処理手順について説明する。図１９は、分析ルールをカスタマ

イズする際の管理マネージャ２０２とモニタエージェント２０３の処理手順を示すフローチャートである。

【００８１】

同図に示すように、ユーザが管理マネージャ２０２のメニューから「分析ルールカスタマイズ」を選択し（ステップＳ１９０１）、分析ルールをカスタマイズするモニタエージェント２０３を指定すると（ステップＳ１９０２）、管理マネージャ２０２は、指定されたモニタエージェント２０３に対して、分析ルールのカスタマイズ可能な部分である分析項目リストを要求する（ステップＳ１９０３）。

【００８２】

そして、この要求を受けたモニタエージェント２０３は、管理マネージャ２０２に対して分析項目リストを送り（ステップＳ１９０４）、管理マネージャ２０２は、分析項目リストを編集する分析項目エディタを起動する（ステップＳ１９０５）。

【００８３】

その後、ユーザは、この分析項目エディタを用いて分析項目リストをカスタマイズし（ステップＳ１９０６）、管理マネージャ２０２は、カスタマイズした分析項目リストをモニタエージェント２０３に配布する（ステップＳ１９０７）。

【００８４】

そして、モニタエージェント２０３は、分析項目リストを更新した後（ステップＳ１９０８）、更新結果を管理マネージャ２０２に返し（ステップＳ１９０９）、管理マネージャ２０２はカスタマイズ結果をユーザに報告する（ステップＳ１９１０）。

【００８５】

次に、対策モジュールの更新手順について説明する。図２０は、対策モジュールの更新手順を示すフローチャートである。同図に示すように、ユーザが、入手した対策モジュールを適当なディレクトリに置き（ステップＳ２００１）、管理マネージャ２０２のメニューから「対策モジュール更新」を選択し（ステップＳ２００２）、新しい対策モジュールのファイルパス名と、対策モジュールを送る

アクションエージェント２０４を指定すると（ステップＳ２００３）、管理マネージャ２０２は、該当するアクションエージェント２０４に対して対策モジュールを配布する（ステップＳ２００４）。

【００８６】

そして、アクションエージェント２０４は、対策モジュールを更新したならば（ステップＳ２００５）、更新結果を管理マネージャ２０２に返し（ステップＳ２００６）、管理マネージャ２０２が更新結果をユーザに報告する（ステップＳ２００７）。

【００８７】

次に、管理マネージャ２０２とモニタエージェント２０３との間で授受される検知通知およびＡＣＫのデータ構造について説明する。図２１は、管理マネージャ２０２とモニタエージェント２０３との間で授受される検知通知およびＡＣＫのデータ構造の一例を示す図である。

【００８８】

同図（ａ）に示すように、モニタエージェント２０３は、エンティティの異常を検知した場合に、管理マネージャ２０２に対して検知通知を送信し、また、モニタエージェント２０３は、この検知通知を受け付けたならば、モニタエージェント２０３に対してＡＣＫを返す。

【００８９】

同図（ｂ）に示すように、この検知通知２１０１は、ＯＰコード、エージェントＩＤ、シーケンス番号、事象識別子、被害識別子、エンティティＩＤ、エンティティログ、時刻および対策パラメータからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、シーケンス番号は、モニタエージェント２０３が検知通知につける通し番号である。また、事象識別子は、モニタエージェント２０３が検知した事象を一意に識別する情報であり、被害識別子は、モニタエージェント２０３が検知した事象によって被害を受けたあるいは受ける可能性があるかどうかを示す情報である。また、エンティティＩＤは、モニタエージェント２０３が異常を検知したエンティティのＩＤであり、エンティティログは、モニタエージェント２０３が検知したエンティティの

ログである。

【００９０】

同図（ｃ）に示すように、ＡＣＫ２１０２は、ＯＰコードとシーケンス番号からなる。なお、このシーケンス番号は、モニタエージェント２０３が検知通知につける通し番号である。

【００９１】

次に、管理マネージャ２０２とアクションエージェント２０４との間で授受される対策依頼および結果通知のデータ構造について説明する。図２２は、管理マネージャ２０２とアクションエージェント２０４との間で授受される対策依頼および結果通知のデータ構造の一例を示す図である。

【００９２】

同図（ａ）に示すように、モニタエージェント２０３は、対策および対策依頼先を決定すると、アクションエージェント２０４に対して対策依頼を送る。一方、アクションエージェント２０４は、この対策依頼を受け取ると、対策依頼で指定された対策を実施し、管理マネージャ２０２に対策結果を返す。

【００９３】

同図（ｂ）に示すように、この対策依頼２２０１は、ＯＰコード、エージェントＩＤ、シーケンス番号、エンティティＩＤ、対策識別子および対策パラメータからなる。ここで、このシーケンス番号は、管理マネージャ２０２が対策依頼につける通し番号であり、対策識別子は、アクションエージェント２０４が保有する対策機能を一意に識別する情報であり、対策パラメータは、モニタエージェント２０３が異常を起こしたエンティティのログをフィールドごとに分割したものである。

【００９４】

同図（ｃ）に示すように、結果通知２２０２は、ＯＰコード、シーケンス番号、エンティティＩＤ、戻り値およびエラーコードからなる。ここで、このシーケンス番号は、管理マネージャ２０２が対策依頼につける通し番号であり、エンティティＩＤは、アクションエージェント２０４が設定を変更したエンティティのＩＤであり、戻り値は、設定変更によりエンティティが返す値である。また、エ

ラーコードは、対策が実施された場合には「E_OK」となり、知らない対策識別子が渡された場合には「E_UNKNOWN」となり、対策パラメータが不足した場合には「E_LESS_ARG」となり、予期しないエラーが発生した場合には「E_UNDEF」となる。

【００９５】

次に、管理マネージャ２０２とモニタエージェント２０３との間で授受されるＤＢ（分析ルール）配布および結果通知のデータ構造について説明する。図２３は、管理マネージャ２０２とモニタエージェント２０３との間で授受されるＤＢ（分析ルール）配布および結果通知のデータ構造の一例を示す図である。

【００９６】

同図（ａ）に示すように、モニタエージェント２０３の分析ルールを更新するために、管理マネージャ２０２は、モニタエージェント２０３に対してＤＢ（分析ルール）を配布する。モニタエージェント２０３は、このＤＢ配布を受け取ると、配布された分析ルールを取り込み、取り込み結果を管理マネージャ２０２に返す。

【００９７】

同図（ｂ）に示すように、このＤＢ配布２３０１は、ＯＰコード、エージェントＩＤおよび分析ルールからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、分析ルールは、配布対象となる分析ルールである。

【００９８】

同図（ｃ）に示すように、結果通知２３０２は、ＯＰコード、エージェントＩＤおよびエラーコードからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布されたルールのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布されたルールが古い場合（同じ判を含む）には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【００９９】

次に、管理マネージャ２０２とモニタエージェント２０３との間で授受されるリスト要求およびリストのデータ構造について説明する。図２４は、管理マネージャ２０２とモニタエージェント２０３との間で授受されるリスト要求およびリストのデータ構造の一例を示す図である。

【０１００】

同図（ａ）に示すように、モニタエージェント２０３の分析項目をカスタマイズするために、管理マネージャ２０２は、モニタエージェント２０３に分析項目リストを要求する。このモニタエージェント２０３は、このリスト要求を受け付けると、分析項目リストを管理マネージャ２０２に返す。

【０１０１】

同図（ｂ）に示すように、このリスト要求２４０１は、ＯＰコードとエージェントＩＤからなり、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤである。

【０１０２】

同図（ｃ）に示すように、リスト２４０２は、ＯＰコード、エージェントＩＤ、分析項目リストおよびエラーコードからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、分析項目リストは、モニタエージェントの現在の分析項目リストであり、エラーコードは、通常は「E_OK」となり、更新中に予期しないエラーが発生した「E_UNDEF」となる。

【０１０３】

次に、管理マネージャ２０２とモニタエージェント２０３との間で授受されるリスト配布および結果通知のデータ構造について説明する。図２５は、管理マネージャ２０２とモニタエージェント２０３との間で授受されるリスト配布および結果通知のデータ構造の一例を示す図である。

【０１０４】

同図（ａ）に示すように、モニタエージェント２０３の分析項目をカスタマイズするために、管理マネージャ２０２は、モニタエージェント２０３に対して分析項目リストを配布する。モニタエージェント２０３は、このリスト配布を受け取ると、配布された分析項目リストを取り込み、取り込み結果を管理マネージャ

２０２に返す。

【０１０５】

同図（ｂ）に示すように、このリスト配布２５０１は、ＯＰコード、エージェントＩＤおよび分析項目リストからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、分析項目リストは、配布対象となる分析項目リストである。

【０１０６】

同図（ｃ）に示すように、結果通知２５０２は、ＯＰコード、エージェントＩＤおよびエラーコードからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布された分析リストのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布された分析リストが古い場合（同じ判を含む）には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【０１０７】

次に、管理マネージャ２０２とアクションエージェント２０４との間で授受される対策配布および結果通知のデータ構造について説明する。図２６は、管理マネージャ２０２とアクションエージェント２０４との間で授受される対策配布および結果通知のデータ構造の一例を示す図である。

【０１０８】

同図（ａ）に示すように、アクションエージェント２０４の対策モジュールを更新するために、管理マネージャ２０２は、アクションエージェント２０４に対して対策モジュールを配布する。アクションエージェント２０４は、この対策モジュールの配布を受け付けると、配布された対策モジュールを取り込み、取り込み結果を管理マネージャ２０２に返す。

【０１０９】

同図（ｂ）に示すように、この対策配布２６０１は、ＯＰコード、エージェントＩＤおよび対策モジュールからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、対策モジュールは、配布対

象となる対策である。

【０１１０】

同図（ｃ）に示すように、結果通知２６０２は、ＯＰコード、エージェントＩＤおよびエラーコードからなる。ここで、このエージェントＩＤは、エージェントを一意に特定するオブジェクトＩＤであり、エラーコードは、更新に成功した場合には「E_OK」となり、配布された対策モジュールのフォーマットを認識できない場合には「E_UNKNOWN」となり、配布された対策モジュールが古い場合（同じ判を含む）には「E_OLD_VER」となり、更新処理中に予期しないエラーが発生した場合には「E_UNDEF」となる。

【０１１１】

次に、図２に示した管理マネージャ２０２がおこなう対策決定処理について説明する。図２７は、図２に示した管理マネージャ２０２がおこなう対策決定処理を説明するための説明図である。

【０１１２】

同図に示す管理マネージャ２０２は、対策プランを用いた対策および対策依頼先の決定をおこなう。ここで、この対策プランとは、同じ事象識別子を持つ対策ルールが複数ある場合に、どの対策ルールを選択するかを決定するためのルールであり、被害識別子、脅威識別子および対策識別子のタプルで構成される。

【０１１３】

具体的には、この管理マネージャ２０２がモニタエージェント２０３から事象識別子を受け取ると（ステップＳ２７０１）、この事象識別子から対策ルールを検索し（ステップＳ２７０２）、脅威識別子を取得する（ステップＳ２７０３）。そして、別途モニタエージェント２０３から被害識別子を取得し（ステップＳ２７０４）、この被害識別子と脅威識別子から対策プランを検索する（ステップＳ２７０５）。

【０１１４】

そして、検索した対策識別子から対策ルールを検索し（ステップＳ２７０６）、対策識別子に基づいてアクションエージェント２０４を選択し（ステップＳ２７０７）、選択したアクションエージェント２０４に対して対策を指示する。

【０１１５】

ここで、この被害識別子とは、モニタエージェント２０３が検知した事象によって、被害を受ける可能性があるかどうかを示す識別子であり、この被害識別子には、「被害あり」、「被害なし」、「判別不能」の３つがある。この被害識別子は、モニタエージェント２０３が異常を検知したときに、管理マネージャ２０２に送る検知通知に含まれる。

【０１１６】

また、脅威識別子とは、モニタエージェント２０３が検知した事象によって受ける可能性がある被害の種類（大きさ）を示す識別子である。この被害の種類は、事象によって決まり、対策ルールに含まれる。

【０１１７】

また、対策識別子は、アクションエージェント２０４で実施できる対策を一意に示す識別子であり、管理マネージャ２０２がアクションエージェント２０４に送る対策依頼に含まれる。なお、対策指示子は、管理マネージャ２０２がどのアクションエージェント２０４に対策依頼を送るかを示す指示子である。

【０１１８】

また、事象識別子は、モニタエージェント２０３が検知した事象を一意に示す識別子である。モニタエージェント２０３が、異常を検知したときに管理マネージャ２０２に送る検知通知に含まれる。

【０１１９】

次に、対策プランの一例について説明する。図２８は、対策プランの一例を示す図である。同図に示す対策プランと対策ルールがある場合には、管理マネージャ２０２は、この対策プランと対策ルールを使って、対策および対策依頼先を決定する。

【０１２０】

たとえば、同図（ａ）に示すように、モニタエージェント２０３が「事象０００１」を検知し、「被害あり」と管理マネージャ２０２に通知した場合には、この管理マネージャ２０２は、「事象０００１」を検索キーとして同図（ｂ）に示す対策ルールを検索する。ここでは、同図（ｂ）に示したように２つの対策ルー

ルがヒットすることになるが、脅威識別子は必ず同じものとなる（ここでは「脅威０００１」となる）。

【０１２１】

そして、管理マネージャ２０２は、「被害あり」、「脅威０００１」を検索キーとして同図（ｃ）に示す対策プランを検索し、対策プランの対策識別子の欄から「対策０００１」を選出する。

【０１２２】

その後、同図（ｄ）に示すように、２つのヒットした対策ルールのうち、「対策０００１」を含むルールを選択し、対策指示子の欄から「ＳＥＲＶＥＲ」を対策依頼先として選出する。なお、モニタエージェント２０３が「事象０００１」を検知し、「被害不明」と管理マネージャ２０２に通知した場合には、対策として「対策０００２」が選出されることになる。

【０１２３】

このように、この対策ルールは、ある事象に対してとり得る可能性がある対策のすべてを列挙したものであり、対策プランとは、列挙された対策ルールを選択するためのルールであり、被害の有無、被害の大きさによって選択する。なお、かかる対策ルールと対策プランを一つにすることもできるが、被害の有無、被害の大きさによって選択する対策をシステムを運用するサイトのポリシーによってカスタマイズできるようにするために、両者を分けている。このため、ユーザは、対策プランをカスタマイズすることができる。

【０１２４】

次に、図２に示した管理マネージャ２０２の機能的な構成について説明する。図２９および図３０は、図２に示した管理マネージャ２０２の機能的な構成を示すブロック図である。

【０１２５】

図２９に示すように、管理マネージャ２０２は、オブジェクト管理部２９０１、状態監視部２９０２、プラン構築部２９０３およびエージェント機能管理部２９０４を有する。

【０１２６】

オブジェクト管理部２９０１は、管理マネージャ２０２、エージェント、エンティティをそれぞれオブジェクトとして管理する機能部であり、対策ルールおよび対策プランは、管理マネージャオブジェクトの属性として管理する。なお、後述する対策決定部は、対策を決定するために、このオブジェクト管理部２９０１が管理する対策ルールおよび対策プランを検索する。

【０１２７】

このオブジェクト管理部２９０１は、オブジェクトの構成を管理しており、後述する対策決定部は、対策依頼先を決定するために、このオブジェクト管理部２９０１が管理する構成情報を参照する。

【０１２８】

状態監視部２９０２は、エージェントの動作状態を確認する機能部である。エージェントに定期的に通信をおこない、通信したときに応答があるか否かでオブジェクト管理部２９０１が管理するエージェントオブジェクトのステータス属性を変更する。

【０１２９】

プラン構築部２９０３は、対策プランをカスタマイズする機能部であり、このプラン構築部２９０３では、カスタマイズした対策プランの管理をオブジェクト管理部２９０１に依頼する。

【０１３０】

エージェント機能管理部２９０４は、モニタエージェント２０３の分析ルールを更新またはカスタマイズする機能部であり、アクションエージェント２０４の対策モジュールについても更新する。

【０１３１】

図３０に示すように、この管理マネージャ２０２は、オブジェクト管理部２９０１、検知通知管理部２９０５、対策決定部２９０６、対策選択部２９０７および対策依頼部２９０８を有する。

【０１３２】

検知通知管理部２９０５は、モニタエージェント２０３から送られてくる検知通知を受信および管理する機能部であり、受信した検知通知を対策決定部２９０

６に出力する。

【０１３３】

対策決定部２９０６は、検知通知管理２９０５から渡された検知通知から、アクションエージェント２０４へ依頼する対策および対策依頼先を決定する機能部である。この対策決定部２９０６は、オブジェクト管理部２９０１が管理する対策ルールと対策プランを検索して、対策および対策依頼先を決定して、対策依頼部２９０８に出力する。この対策決定部２９０６は、対策および対策依頼先を複数選び出し、対策選択部２９０７に対策のユーザ選択を依頼する。

【０１３４】

対策選択部２９０７は、対策決定部２９０６から渡された複数の対策をユーザに報告し、ユーザに選択を依頼する機能部である。また、ユーザから対策復元要求を受け付け、対策を元に戻す。

【０１３５】

対策依頼部２９０８は、対策決定部２９０６から渡された対策依頼先が示すアクションエージェント２０４に対して対策決定部２９０６から受け付けた対策を依頼する機能部である。この対策依頼部２９０８は、アクションエージェント２０４の結果通知を受けて、ユーザに対策結果を通知する。また、対策によるエンティティの状態変化を示す対策依頼若しくは対策結果の管理をオブジェクト管理部２９０１に依頼する。

【０１３６】

次に、上記オブジェクト管理部２９０１が管理するオブジェクトの一例について説明する。図３１は、管理マネージャオブジェクトを示す図であり、図３２は、エージェントオブジェクトを示す図であり、図３３は、エンティティオブジェクトを示す図である。

【０１３７】

図３１に示すように、管理マネージャオブジェクトには、管理マネージャ２０２、対策ルール、対策プラン、ログフォーマット定義、エージェント認定リスト、状態監視、モニタエージェント２０３およびアクションエージェント２０４に係るものがある。

【０１３８】

また、図３２に示すように、エージェントオブジェクトには、エージェント、エンティティおよび管理マネージャ２０２に係るものがあり、図３３に示すように、エンティティオブジェクトには、エンティティ、ＦＷエンティティ、モニタエージェント２０３、アクションエージェント２０４、対策履歴およびエンティティ固有情報に係るものがある。

【０１３９】

なお、このオブジェクト管理部２９０１は、オブジェクトの属性値を定義するオブジェクト定義機能、オブジェクトを削除するオブジェクト削除機能、オブジェクトの属性値を参照するオブジェクト参照機能、オブジェクトの属性値を変更するオブジェクト変更機能、並びに、ユーザが作成されたファイルを置くだけでエージェントの設定を済ませることができるエージェント設定ファイル作成補助機能などを有する。

【０１４０】

次に、図３０に示した対策決定部２９０６の動作についてさらに詳細に説明する。図３４は、図３０に示した対策決定部２９０６による対策決定までの処理手順を示すフローチャートである。

【０１４１】

同図に示すように、管理マネージャ２０２は、対策ルールを参照して「脅威識別子」を取得するとともに（ステップＳ３４０１）、対策プランを参照して「対策識別子」を取得する（ステップＳ３４０２）。

【０１４２】

そして、対策識別子がＯＲ結合の場合には、ユーザに対策の選択を依頼し（ステップＳ３４０３）、ユーザが対策を選択する（ステップＳ３４０４）。その後、管理マネージャ２０２は、対策および対策依頼先を決定し（ステップＳ３４０５）、アクションエージェント２０４の動作状態を確認する（ステップＳ３４０６）。

【０１４３】

次に、図３０に示した対策決定部２９０６の構成について説明する。図３５は

、図３０に示した対策決定部２９０６の構成を示す機能ブロック図である。同図に示すように、この対策決定部２９０６は、検知通知管理部２９０５、オブジェクト管理部２９０１、対策依頼部２９０８および対策選択部２９０７の間に介在し、対策決定機能制御部３５０１と、対策ルール検索部３５０２と、対策プラン検索部３５０３と、状態確認部３５０４と、対策決定待ちキュー管理部３５０５と、対策決定待ちキュー３５０６とからなる。

【０１４４】

対策決定機能制御部３５０１は、対策決定機能を制御する機能部であり、対策ルール検索部３５０２は、対策ルールを検索する機能部であり、対策プラン検索部３５０３は、対策プランを検索する機能部であり、状態確認部３５０４は、状態確認をおこなう機能部であり、対策決定待ちキュー管理部３５０５は、対策決定待ちキュー３５０６を管理する機能部である。

【０１４５】

次に、レポーティング機能について説明する。図３６は、レポーティング機能を説明するための説明図である。同図に示すように、監視対象を検知エンジンで検知する際に、実装情報３６０１、運用管理情報３６０２およびセキュリティ情報３６０３に基づいて判定をおこない、検知通知をおこなう。すなわち、監視対象サイトの情報（構成、稼働中サービス、セキュリティ機能など）をもとに、多面的な運用状況を判定して報告している。

【０１４６】

また、かかる実装情報３６０１、運用管理情報３６０２およびセキュリティ情報３６０３は、図３７に示すように、防御策を判定する際にも用いられており、防御策リストから防御策を判定する際に、これらの情報を参照して多面的に防御策を選択し、状況に応じた動的な防御を実施している。ここで実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能である。

【０１４７】

さらに、図３８に示すように、これらの実装情報３６０１、運用管理情報３６０２およびセキュリティ情報３６０３は、プロトコル階層間のフィルタとしても

利用される。すなわち、ＩＰ層とＴＣＰ層との間、ＴＣＰ層とＨＴＴＰ層の間、ＨＴＴＰ層とＭＩＭＥデータの間、ＭＩＭＥデータとＣＧＩ－ＡＰの間のフィルタとして用いることにより、各階層の不正アクセス手口を限定し、解析・検知コストの軽減を図ることができる。

【０１４８】

また、正常なリクエスト以外を他層に渡さないようフィルタリングすることにより、攻撃に対する防御を実現することができる。さらに、監視対象に関する情報（システム構成、稼働サービス、セキュリティ機能）を参考にし、判定処理の信頼性や妥当性を向上させることもできる。

【０１４９】

次に、これらの実装情報３６０１、運用管理情報３６０２およびセキュリティ情報３６０３を用いた統合連携管理について説明する。図３９は、実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図である。

【０１５０】

同図に示すように、セキュリティ情報３６０３は不正手口へとつながり、運用管理情報はサイト情報へとつながり、実装情報はソフト情報へとつながる。ここで、これらの不正手口、サイト情報およびソフト情報は、検知、被害予想・把握、防御・回避・復旧をおこなううえで重要な役割を果たしている。

【０１５１】

換言すれば、検知（攻撃検知、予兆検知、攻撃予知）をおこなうためには、不正手口、サイト情報およびソフト情報といった総合的な情報が必要であり、また被害予想・把握をおこなったり、防御・回避・復旧をおこない際にも同様の総合的な情報が必要となる。このため、本実施の形態では、実装情報３６０１、運用管理情報３６０２およびセキュリティ情報３６０３を用いた統合連携制御をおこなっている。

【０１５２】

上述してきたように、本実施の形態によれば、モニタエージェント２０３でエンティティのログを分析し、異常の予兆を検知した場合には、管理マネージャ２

０２に通知する。そして、この管理マネージャ２０２は、データベース２０１などに基づいて対策および対策依頼先を決定し、対策依頼先であるアクションエージェント２０４に該当する対策を実施させるよう構成したので、サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることができる。

【０１５３】

（付記１）　通信要求を監視する通信要求監視手段と、前記通信要求監視手段から通知された情報に基づいて対策を選択する管理手段と、前記管理手段からの指示に応答して対策を実施する実施手段とを有し、

前記管理手段は、

前記通信要求監視手段からの通知内容と前記実施手段が実施する対策とを対応づけて管理するデータベースと、

前記データベースに基づいて対策を選択する選択手段と、

を備えたことを特徴とする情報管理システム。

【０１５４】

（付記２）　攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集手段と、前記情報収集手段により収集整理された情報を前記データベースに反映する反映手段と、をさらに備えたことを特徴とする付記１に記載の情報管理システム。

【０１５５】

（付記３）　前記選択手段は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする付記１または２に記載の情報管理システム。

【０１５６】

（付記４）　前記実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能であることを特徴とする付記３に記載の情報管理システム。

【０１５７】

（付記５）　複数の通信要求監視手段、管理手段および実施手段をそれぞれ

備えたことを特徴とする付記１～４のいずれか一つに記載の情報管理システム。

【０１５８】

（付記６）　前記複数の通信要求監視手段、管理手段および実施手段が同機種または異機種間でそれぞれ相互に連携して情報交換をおこなうことを特徴とする付記５に記載の情報管理システム。

【０１５９】

（付記７）　前記通信要求監視手段により通知される情報および／または前記管理手段により選択される対策に重み付けをおこなうことを特徴とする付記１～６のいずれか一つに記載の情報管理システム。

【０１６０】

（付記８）　前記重み付けする重み係数は、ユーザによって任意に設定できることを特徴とする付記７に記載の情報管理システム。

【０１６１】

（付記９）　前記重み付けする重み係数は、前記実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定されることを特徴とする付記７に記載の情報管理システム。

【０１６２】

（付記１０）　前記データベースは、前記通信要求監視手段により通知される情報を時系列で保持し、前記選択手段は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする付記１～９のいずれか一つに記載の情報管理システム。

【０１６３】

（付記１１）　前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成手段をさらに備えたことを特徴とする付記１～１０のいずれか一つに記載の情報管理システム。

【０１６４】

（付記１２）　前記サイトマップ生成手段により生成されたサイトマップに基づいて、監視対象となる通信の種類および／または時間を前記複数の通信要求

監視手段に通知する監視条件通知手段をさらに備えたことを特徴とする付記１～１０のいずれか一つに記載の情報管理システム。

【０１６５】

（付記１３）　前記管理手段は、ネットワークに所在するサイトに対してリクエストを発し、該リクエストに応答して返信される情報に基づいて前記データベースを自動更新することを特徴とする付記１～１２のいずれか一つに記載の情報管理システム。

【０１６６】

（付記１４）　前記リクエストは、ユーザの要求に応答しておこなうことを特徴とする付記１３に記載の情報管理システム。

【０１６７】

（付記１５）　前記管理手段は、ネットワークに所在するサイトから自動的に送信される情報に基づいて前記データベースを自動更新することを特徴とする付記１～１２のいずれか一つに記載の情報管理システム。

【０１６８】

（付記１６）　ネットワークに所在するサイトから自動的に送信される情報をユーザの要求に応答して前記データベースに取り込むことを特徴とする付記１５に記載の情報管理システム。

【０１６９】

（付記１７）　システムの脆弱性を示す脆弱性呈示手段と、前記脆弱性呈示手段に対する攻撃に関する情報を収集する情報収集手段と、をさらに備えたことを特徴とする付記１～１６のいずれか一つに記載の情報管理システム。

【０１７０】

（付記１８）　通信内容の発信元を調査する調査手段と、前記調査手段による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定手段と、をさらに備えたことを特徴とする付記１～１７のいずれか一つに記載の情報管理システム。

【０１７１】

（付記１９）　攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、

前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに備えたことを特徴とする付記１～１８のいずれか一つに記載の情報管理システム。

【０１７２】

（付記２０）　通信要求を監視部によって監視する通信要求監視工程と、

前記通信要求監視工程により通知される通知知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、

前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、

を含んだことを特徴とする情報管理方法。

【０１７３】

（付記２１）　攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集する情報収集工程と、前記情報収集工程により収集整理された情報を前記データベースに反映する反映工程と、をさらに含んだことを特徴とする付記２０に記載の情報管理方法。

【０１７４】

（付記２２）　前記選択工程は、前記データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することを特徴とする付記２０または２１に記載の情報管理方法。

【０１７５】

（付記２３）　前記実装情報、運用管理情報および／またはセキュリティ情報のいずれに基づいて対策を選択するかは、ユーザの選択に応じて設定変更可能であることを特徴とする付記２２に記載の情報管理方法。

【０１７６】

（付記２４）　複数の監視部、管理部および実施部をそれぞれ設けたことを特徴とする付記２０～２３のいずれか一つに記載の情報管理方法。

【０１７７】

（付記２５）　前記複数の監視部、管理部および実施部が同機種または異機種間でそれぞれ相互に連携して情報交換をおこなうことを特徴とする付記２４に記載の情報管理方法。

【０１７８】

（付記２６）　前記監視部により通知される情報および／または前記管理部により選択される対策に重み付けをおこなうことを特徴とする付記２０～２５のいずれか一つに記載の情報管理方法。

【０１７９】

（付記２７）　前記重み付けする重み係数は、ユーザによって任意に設定できることを特徴とする付記２６に記載の情報管理方法。

【０１８０】

（付記２８）　前記重み付けする重み係数は、前記実装情報、運用管理情報および／またはセキュリティ情報に基づいて設定されることを特徴とする付記２６に記載の情報管理方法。

【０１８１】

（付記２９）　前記データベースは、前記監視部により通知される情報を時系列で保持し、前記選択工程は、前記データベースに記憶した時系列の情報に基づいて対策を選択することを特徴とする付記２０～２８のいずれか一つに記載の情報管理方法。

【０１８２】

（付記３０）　前記複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するサイトマップ生成工程をさらに含んだことを特徴とする付記２０～２９のいずれか一つに記載の情報管理方法。

【０１８３】

（付記３１）　前記サイトマップ生成工程により生成されたサイトマップに基づいて、監視対象となる通信の種類および／または時間を前記複数の監視部に通知する監視条件通知工程をさらに含んだことを特徴とする付記２０～２９のいずれか一つに記載の情報管理方法。

【０１８４】

（付記３２）　前記管理部が、ネットワークに所在するサイトに対してリクエストを発し、該リクエストに応答して返信される情報に基づいて前記データベースを自動更新することを特徴とする付記２０～３１のいずれか一つに記載の情

報管理方法。

【０１８５】

（付記３３）　前記リクエストは、ユーザの要求に応答しておこなうことを特徴とする付記３２に記載の情報管理方法。

【０１８６】

（付記３４）　前記管理部が、ネットワークに所在するサイトから自動的に送信される情報に基づいて前記データベースを自動更新することを特徴とする付記２０～３１のいずれか一つに記載の情報管理方法。

【０１８７】

（付記３５）　ネットワークに所在するサイトから自動的に送信される情報をユーザの要求に応答して前記データベースに取り込むことを特徴とする付記３４に記載の情報管理方法。

【０１８８】

（付記３６）　システムの脆弱性を示す脆弱性呈示工程と、前記脆弱性呈示工程に対する攻撃に関する情報を収集する情報収集工程と、をさらに含んだことを特徴とする付記２０～３５のいずれか一つに記載の情報管理方法。

【０１８９】

（付記３７）　通信内容の発信元を調査する調査工程と、前記調査工程による調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定する判定工程と、をさらに含んだことを特徴とする付記２０～３６のいずれか一つに記載の情報管理方法。

【０１９０】

（付記３８）　攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、前記攻撃対象サイトへの攻撃を回避させるおとりサイトをさらに含んだことを特徴とする付記２０～３７のいずれか一つに記載の情報管理方法。

【０１９１】

（付記３９）　通信要求を監視部によって監視する通信要求監視工程と、

前記通信要求監視工程により通知される通知知内容と実施する対策とを対応づけて管理するデータベースに基づいて管理部が対策を選択する選択工程と、

前記管理工程からの指示に応答して実施部が対策を実施する実施工程と、

をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【０１９２】

【発明の効果】

以上説明したように、請求項１、９および１０の発明によれば、データベース内に通知内容と対策を対応づけて保持しておき、通信要求監視手段が通信要求を監視して異常を検知して管理手段に通知すると、この管理手段が、データベースから対策を選択して、実施手段に対策を実行させるよう構成したので、対策を効率良く実行することができ、もって、実際の攻撃に適切な対策を施して被害の極小化を図ることができる。

【０１９３】

また、請求項２の発明によれば、攻撃事象若しくは漏洩事象の進行過程における２以上の通信の種類、内容、順序および時間間隔に係る情報を収集し、収集整理された情報をデータベースに反映するよう構成したので、データベースの内容を充実させ、より適切な対策を選択することができる。

【０１９４】

また、請求項３の発明によれば、データベース並びに実装情報、運用管理情報および／またはセキュリティ情報に基づいて多面的に対策を選択することとしたので、データベースのみならずシステムを取り巻く環境を考慮した上で妥当な対策を未然に実行し、もって被害を極小化することができる。

【０１９５】

また、請求項４の発明によれば、データベースが通信要求監視手段により通知される情報を時系列で保持し、このデータベースに記憶した時系列の情報に基づいて対策を選択するよう構成したので、時系列的な情報を用いて対策を選択することができる。

【０１９６】

また、請求項５の発明によれば、複数の通信要求監視手段により通知される情報に基づいて、サイトの空間的配置を示すサイトマップを生成するよう構成した

ので、空間的な情報を用いて対策を選択することができる。

【０１９７】

また、請求項６の発明によれば、システムの脆弱性を明示的に呈示し、この脆弱箇所に対する攻撃に関する情報を収集するよう構成したので、悪意者による攻撃手法を把握することができる。

【０１９８】

また、請求項７の発明によれば、通信内容の発信元を調査した調査結果に基づいてサイトが悪意者による踏み台とされているか否かを判定するよう構成したので、踏み台とされているサイトを効率良く特定することができる。

【０１９９】

また、請求項８の発明によれば、攻撃対象となる攻撃対象サイトと異なる所在へ通信を導き、この攻撃対象サイトへの攻撃を回避させるおとりサイトを設けるよう構成したので、攻撃対象サイトの保全を図るとともに攻撃手法を把握することができる。

【図面の簡単な説明】

【図１】

この発明の実施の形態に係る全体システムに採用した各種技術を説明するための説明図である。

【図２】

本実施の形態に係る情報管理システムの基本構成を示すブロック図である。

【図３】

モニタエージェントおよびアクションエージェントを複数設けた場合の構成を示すブロック図である。

【図４】

管理マネージャが重み付けしたデータＡと重み付けした対策Ｂを対応づけて保持した場合を示すブロック図である。

【図５】

図４に示したモニタエージェントの構成を示すブロック図である。

【図６】

図２に示した管理マネージャを説明するための説明図である。

【図７】

図２に示した管理マネージャによる物理マップの作成を説明するための説明図である。

【図８】

図２に示した管理マネージャからモニタエージェントに対するフィードバックを説明するための説明図である。

【図９】

モジュール間の相互情報参照を説明するための説明図である。

【図１０】

図２に示したデータベースの自動更新（ＰＵＬＬ型）を説明するための説明図である。

【図１１】

図２に示したデータベースの自動更新（ＰＵＳＨ型）を説明するための説明図である。

【図１２】

人手を介した場合を含むデータベースの自動更新（ＰＵＬＬ型）を説明するための説明図である。

【図１３】

人手を介した場合を含むデータベースの自動更新（ＰＵＳＨ型）を説明するための説明図である。

【図１４】

モニタエージェントが異常を検知してからアクションエージェントが対策を実施するまでの処理手順を示すフローチャートである。

【図１５】

エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャートである。

【図１６】

図２に示した管理マネージャにおける対策ルールの更新手順を説明するための

説明図である。

【図１７】

図２に示した管理マネージャにおいて対策プランをカスタマイズする際の処理手順を示すフローチャートである。

【図１８】

分析ルールを更新する際の管理マネージャとモニタエージェントの処理手順を示すフローチャートである。

【図１９】

分析ルールをカスタマイズする際の管理マネージャとモニタエージェントの処理手順を示すフローチャートである。

【図２０】

対策モジュールの更新手順を示すフローチャートである。

【図２１】

管理マネージャとモニタエージェントとの間で授受される検知通知およびＡＣＫのデータ構造の一例を示す図である。

【図２２】

管理マネージャとアクションエージェントとの間で授受される対策依頼および結果通知のデータ構造の一例を示す図である。

【図２３】

管理マネージャとモニタエージェントとの間で授受されるＤＢ（分析ルール）配布および結果通知のデータ構造の一例を示す図である。

【図２４】

管理マネージャとモニタエージェントとの間で授受されるリスト要求およびリストのデータ構造の一例を示す図である。

【図２５】

管理マネージャとモニタエージェントとの間で授受されるリスト配布および結果通知のデータ構造の一例を示す図である。

【図２６】

管理マネージャとアクションエージェントとの間で授受される対策配布および

結果通知のデータ構造の一例を示す図である。

【図２７】

図２に示した管理マネージャがおこなう対策決定処理を説明するための説明図である。

【図２８】

対策プランの一例を示す図である。

【図２９】

図２に示した管理マネージャの機能的な構成を示すブロック図である。

【図３０】

図２に示した管理マネージャの機能的な構成を示すブロック図である。

【図３１】

管理マネージャオブジェクトを示す図である。

【図３２】

エージェントオブジェクトを示す図である。

【図３３】

エンティティオブジェクトを示す図である。

【図３４】

図３０に示した対策決定部による対策決定までの処理手順を示すフローチャートである。

【図３５】

図３０に示した対策決定部の構成を示す機能ブロック図である。

【図３６】

レポーティング機能を説明するための説明図である。

【図３７】

実装情報などを用いた多面的な防御策選択を説明するための説明図である。

【図３８】

実装情報などをプロトコル階層間のフィルタとして用いる概念を説明するための説明図である。

【図３９】

実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図である。

【符号の説明】

１０１　攻撃者（悪玉ハッカー）

１０２　おとりサーバ

１０３　ＵＧ系サイト群（善玉ハッカー）

１０４　被害サーバ

１０５　事例データベース

１０６　パケットモニタ群

１０７　踏み台群

１０８　防御対象サーバ

１０９　おとりサーバ

２０１　データベース

２０２　管理マネージャ

２０３　モニタエージェント

２０３ａ　データ解析部

２０３ｂ　データ分析部

２０３ｃ　データスタック

２０３ｄ　重みテーブル

２０３ｅ　判定処理部

２０３ｆ　通知部

２０４　アクションエージェント

２０５　システム構成

２０６　運用状況

２０７　モジュール

２０８　サイトの物理マップ

１００１　コレクタ部

１００２　セレクションデータ

１００３　ネットワーク

１００４　タイマ

１００５　フォーマッタ

１００６　ライタ

１００７　ユーザインターフェース

２１０１　検知通知

２１０２　ＡＣＫ

２２０１　対策依頼

２２０２　結果通知

２３０１　ＤＢ配布

２３０２　結果通知

２４０１　リスト要求

２４０２　リスト

２５０１　リスト配布

２５０２　結果通知

２６０１　対策配布

２６０２　結果通知

２９０１　オブジェクト管理部

２９０２　状態監視部

２９０３　プラン構築部

２９０４　エージェント機能管理部

２９０５　検知通知管理部

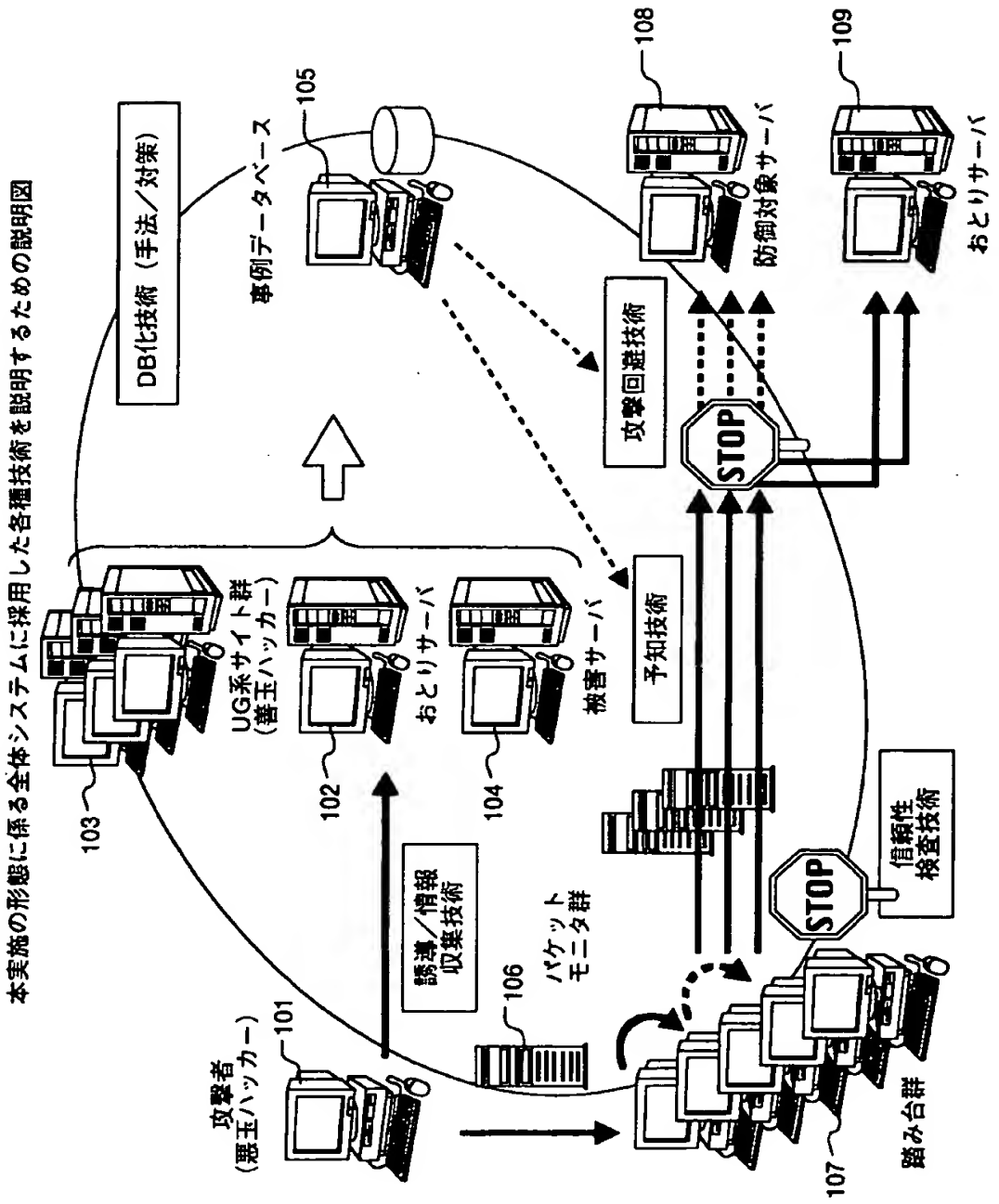
２９０６　対策決定部

２９０７　対策選択部

２９０８　対策依頼部

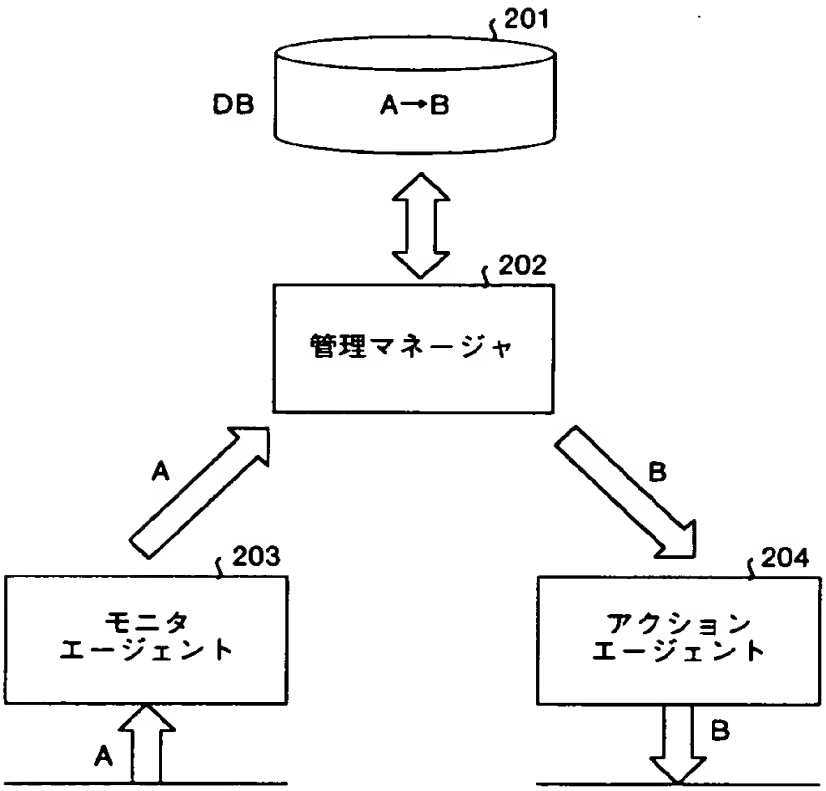
【書類名】　　図面

【図１】


本実施の形態に係る全体システムに採用した各種技術を説明するための説明図
DB化技術（手法／対策）
事例データベース
105
108
109
防御対象サーバ
おとりサーバ
攻撃回避技術
STOP
UG系サイト群
(善玉ハッカー)
おとりサーバ
被害サーバ
予知技術
103
102
104
誘導／情報
収集技術
パケット
モニタ群
106
信頼性
検査技術
STOP
攻撃者
(悪玉ハッカー)
101
踏み台群
107

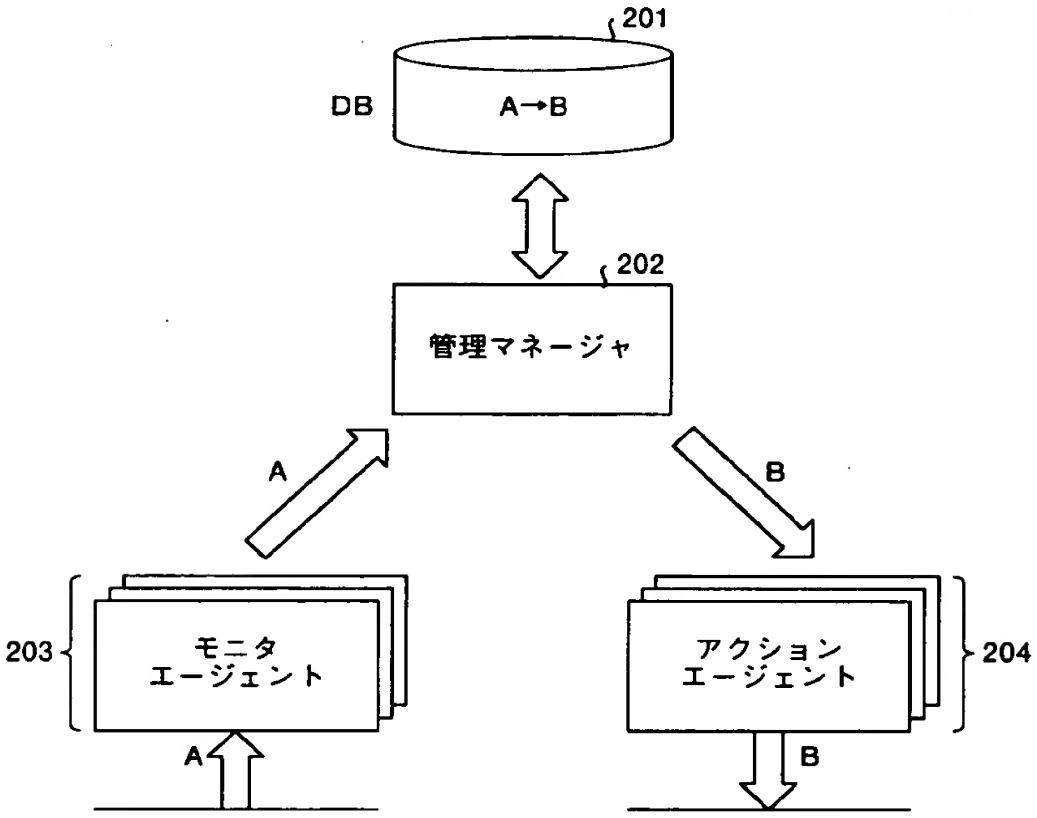
【図２】

本実施の形態に係る情報管理システムの基本構成を示すブロック図



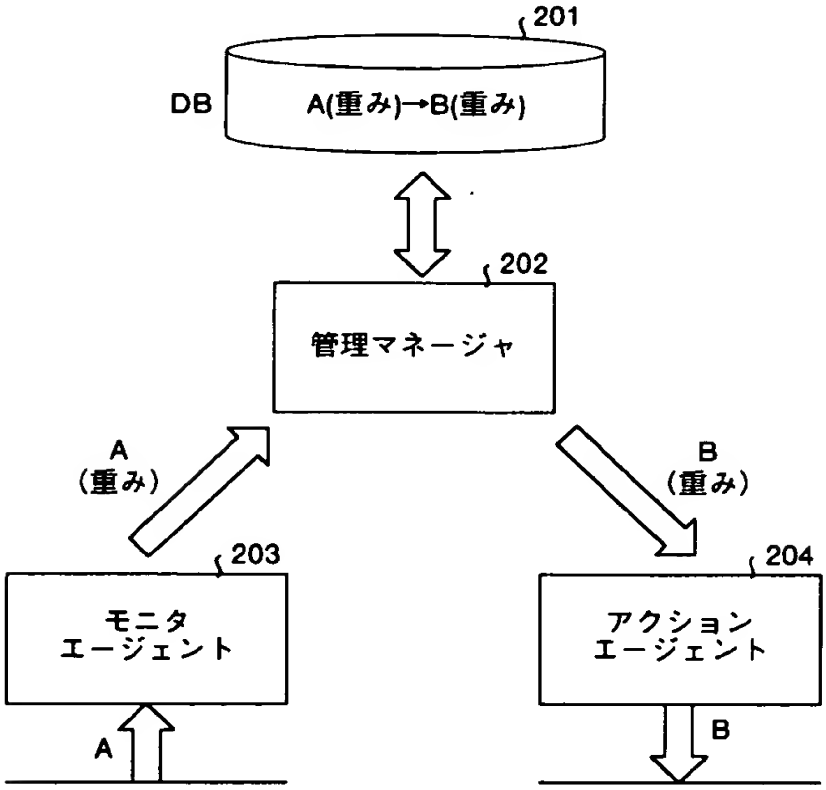
【図３】

モニタエージェントおよび
アクションエージェントを複数設けた場合の構成を示すブロック図



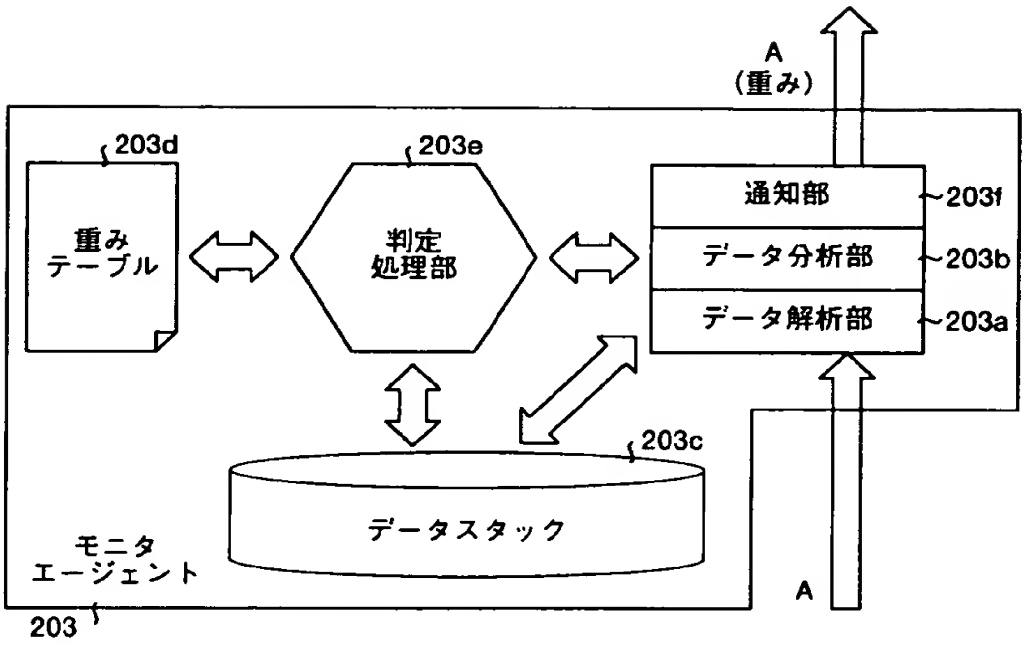
【図４】

管理マネージャが重み付けしたデータAと
重み付けした対策Bを対応づけて保持した場合を示すブロック図



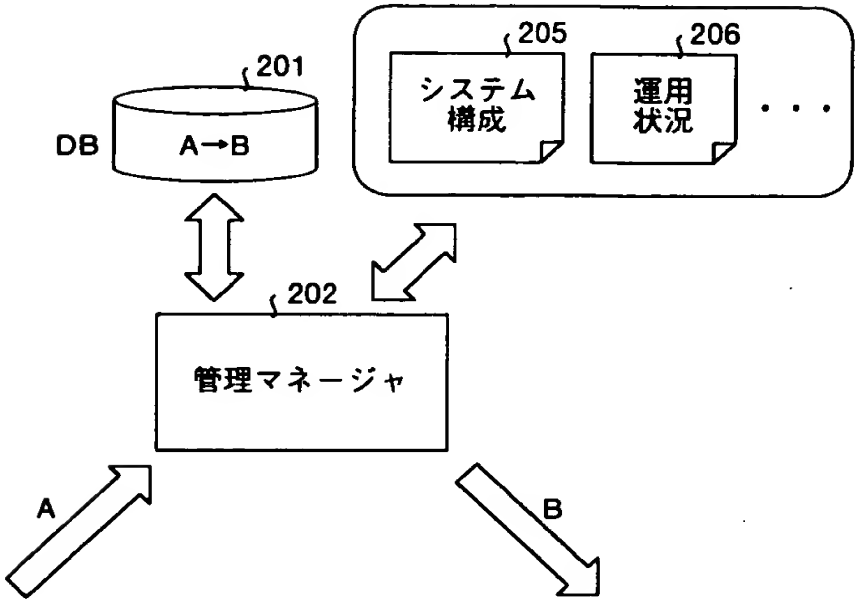
【図５】

モニタエージェントの構成を示すブロック図



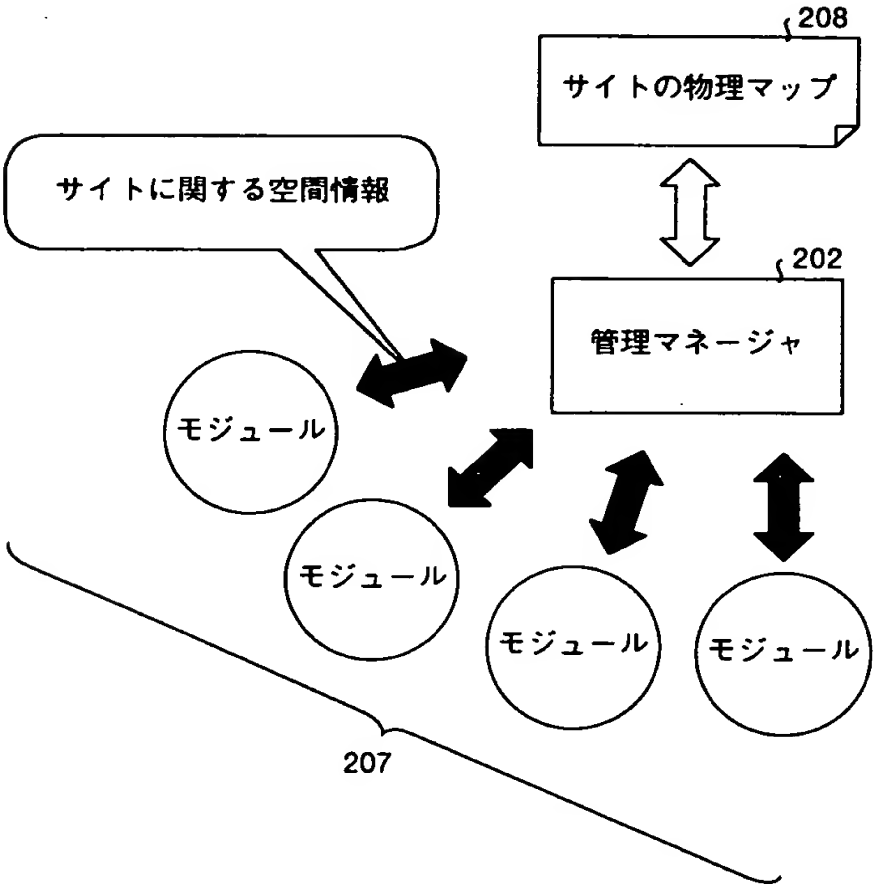
【図６】

管理マネージャを説明するための説明図



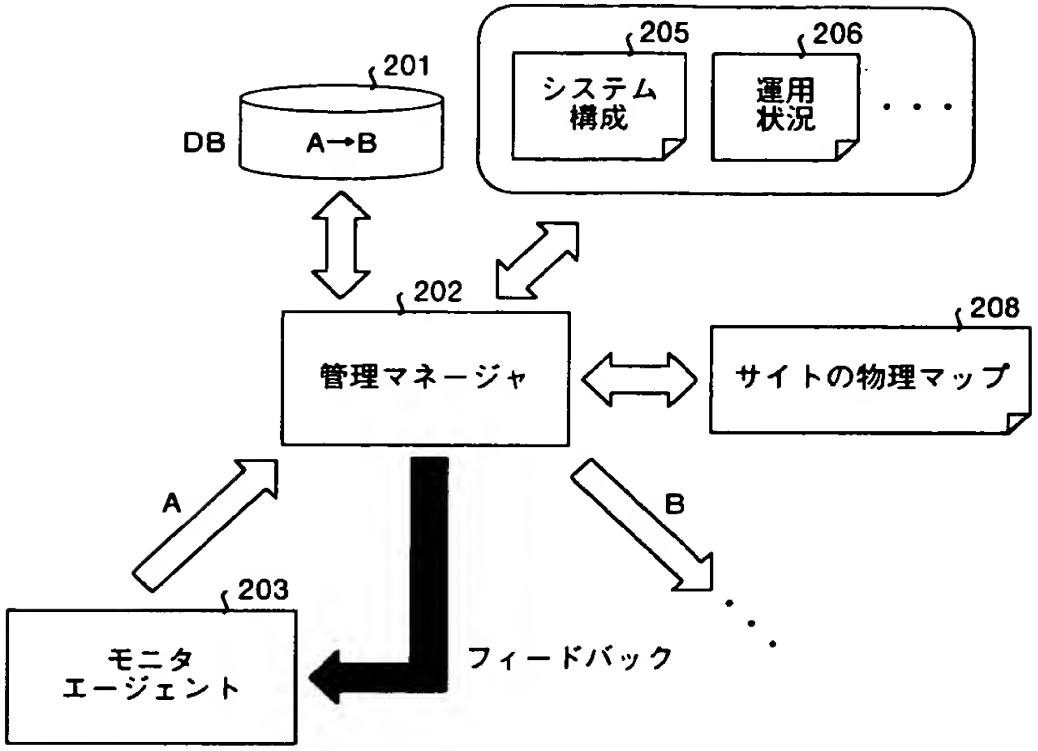
【図７】

管理マネージャによる物理マップの作成を説明するための説明図



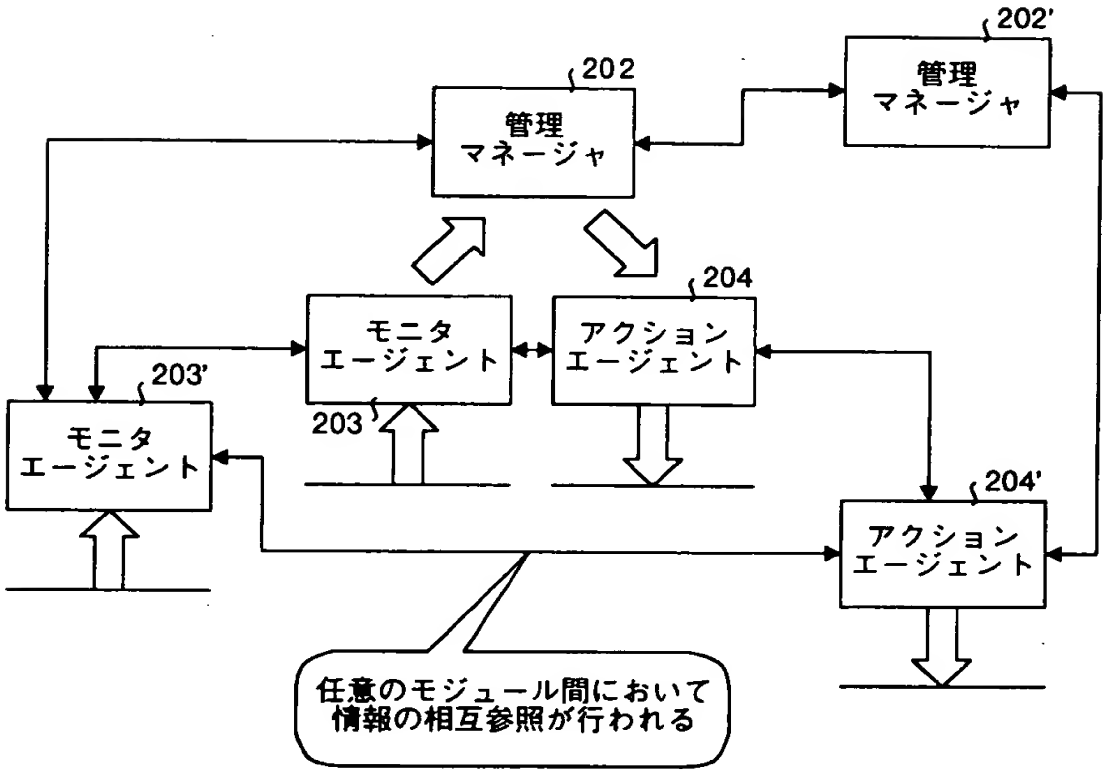
【図８】

管理マネージャからモニタエージェントに対する
フィードバックを説明するための説明図



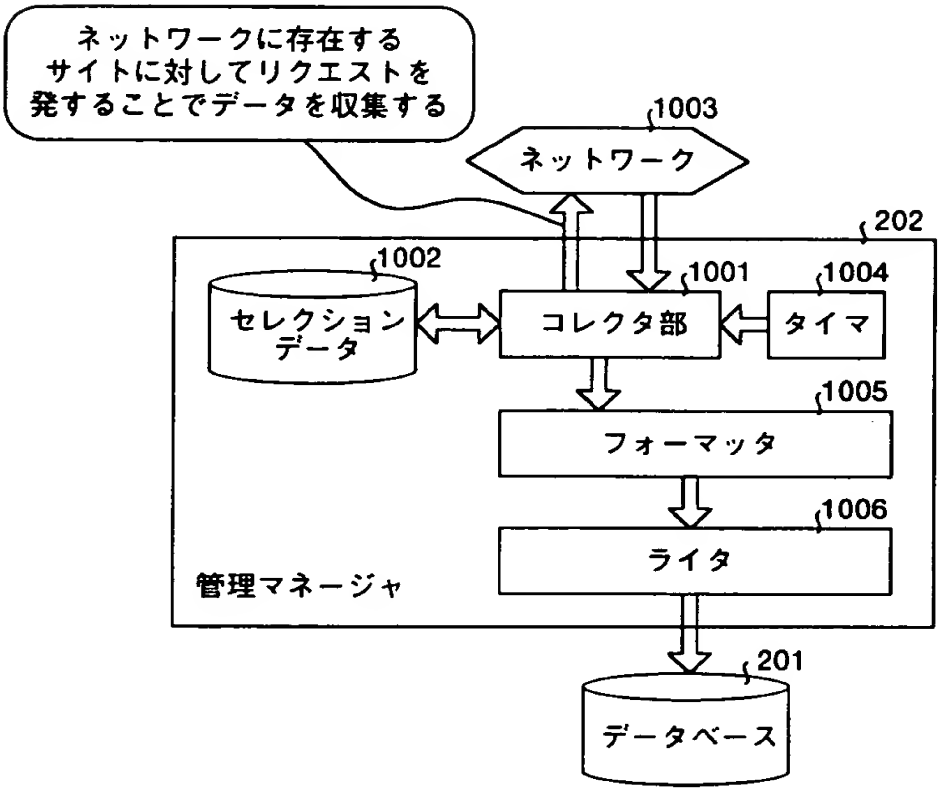
【図９】

モジュール間の相互情報参照を説明するための説明図



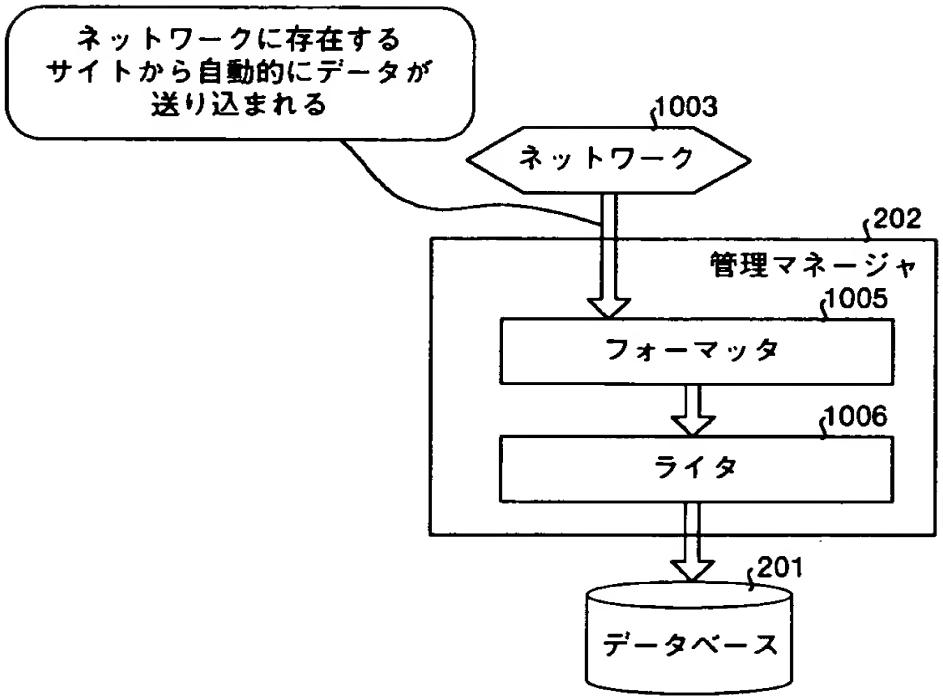
【図１０】

データベースの自動更新（PULL型）を説明するための説明図



【図１１】

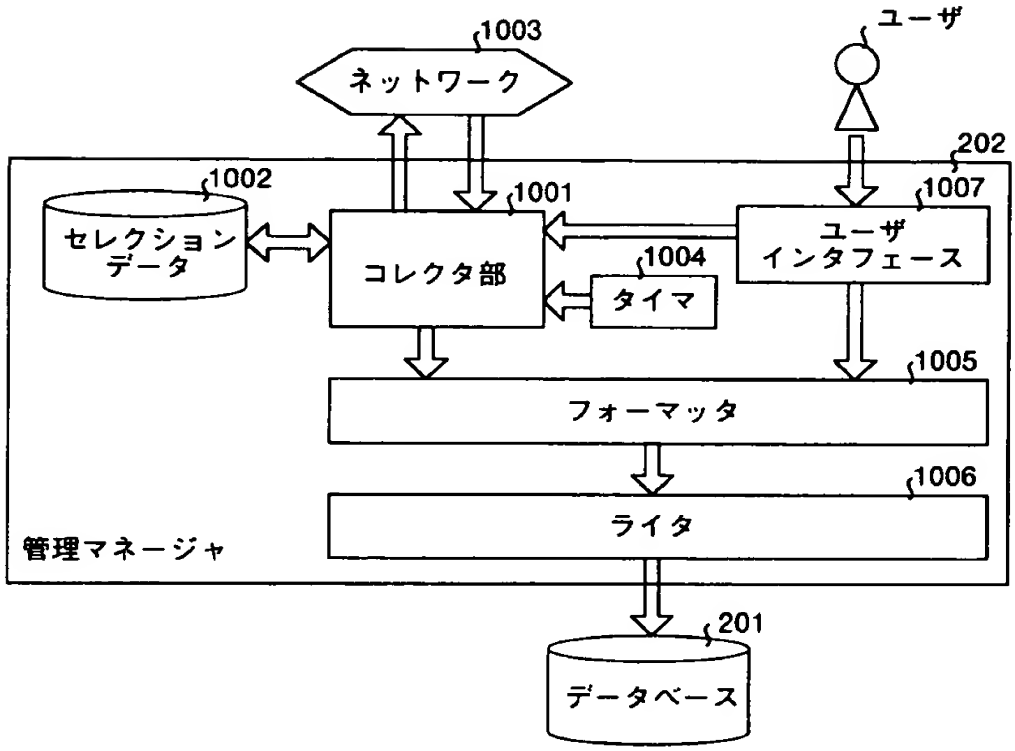
データベースの自動更新（PUSH型）を説明するための説明図



出証特２００１－３０５２４９３

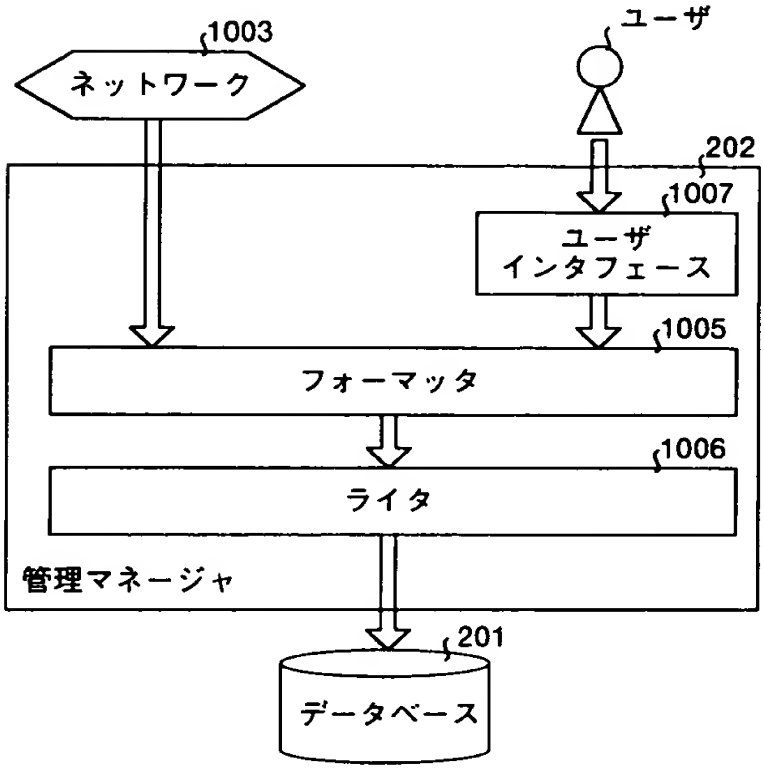
【図１２】

人手を介した場合を含むデータベースの自動更新（PULL型）を
説明するための説明図



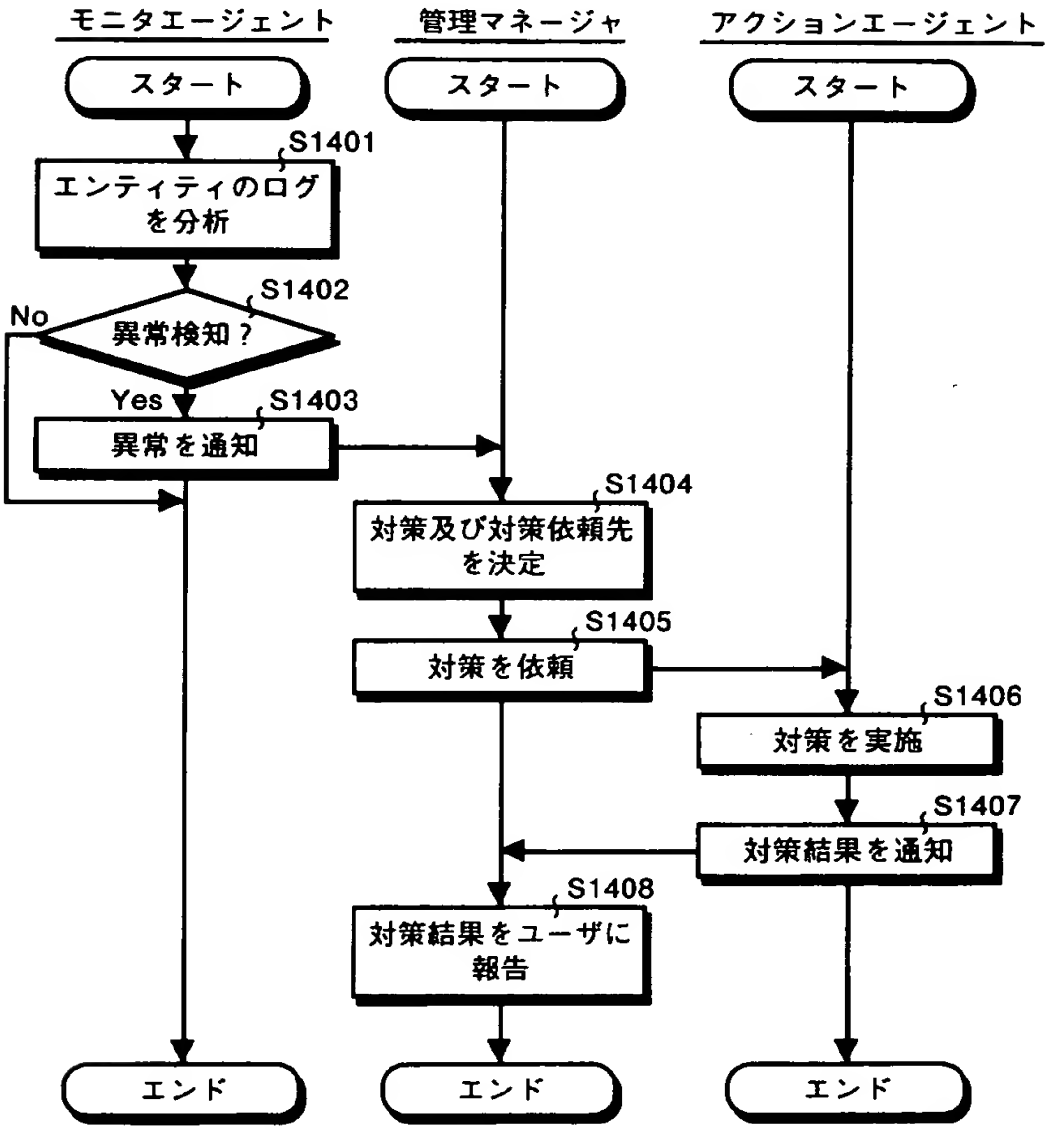
【図１３】

人手を介した場合を含むデータベースの自動更新（PUSH型）を説明するための説明図



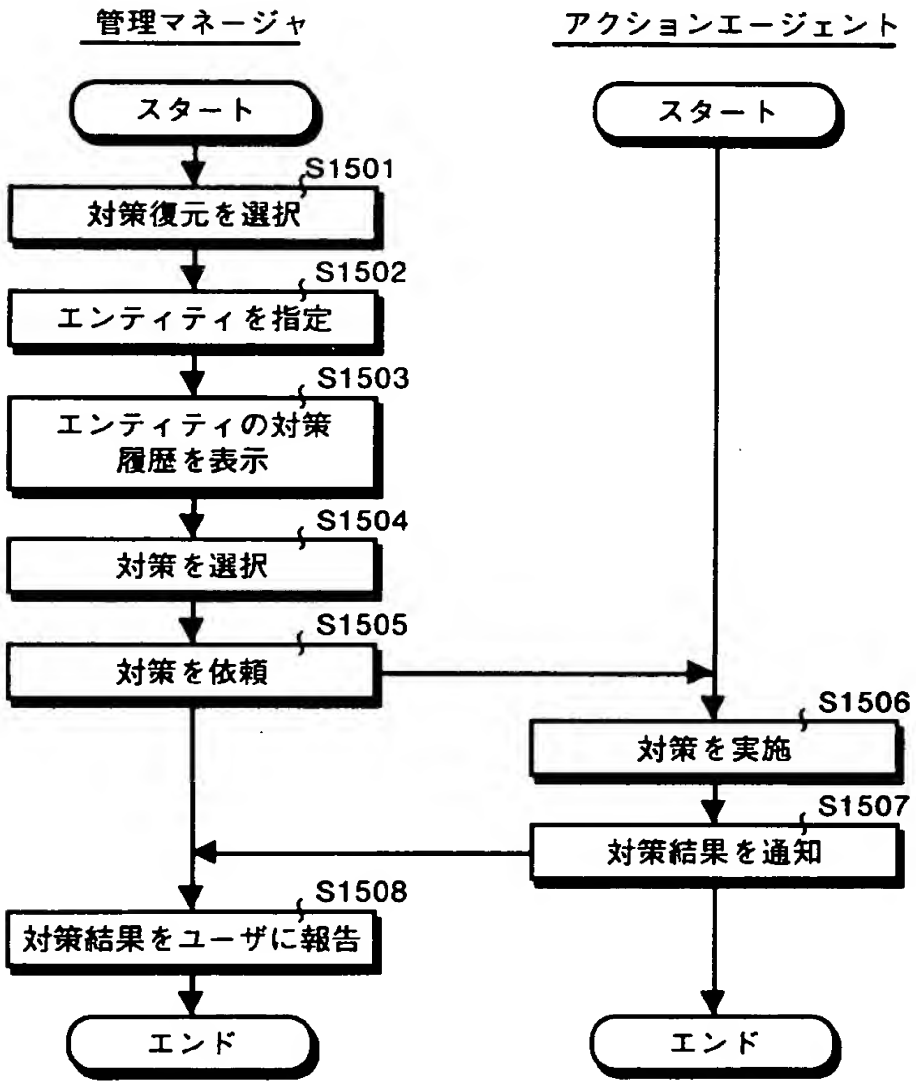
【図１４】

モニタエージェントが異常を検知してからアクションエージェントが対策を実施するまでの処理手順を示すフローチャート



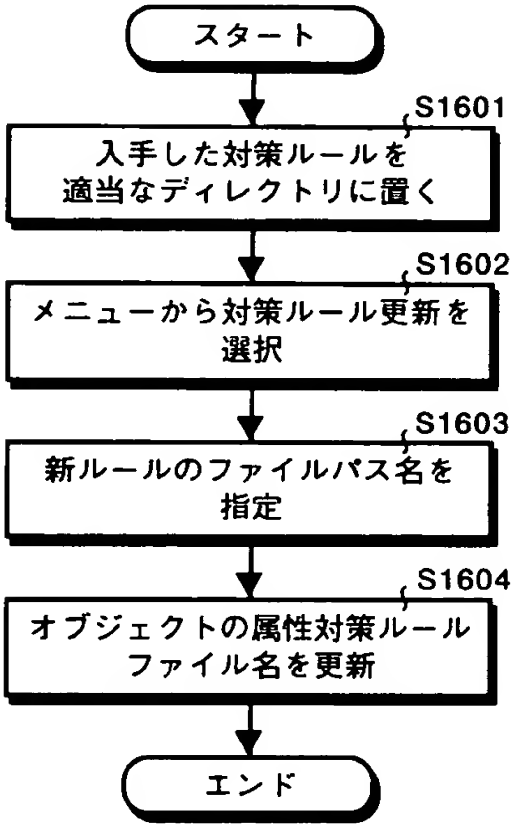
【図１５】

エンティティを対策実施前の状態に戻す場合の処理手順を示すフローチャート



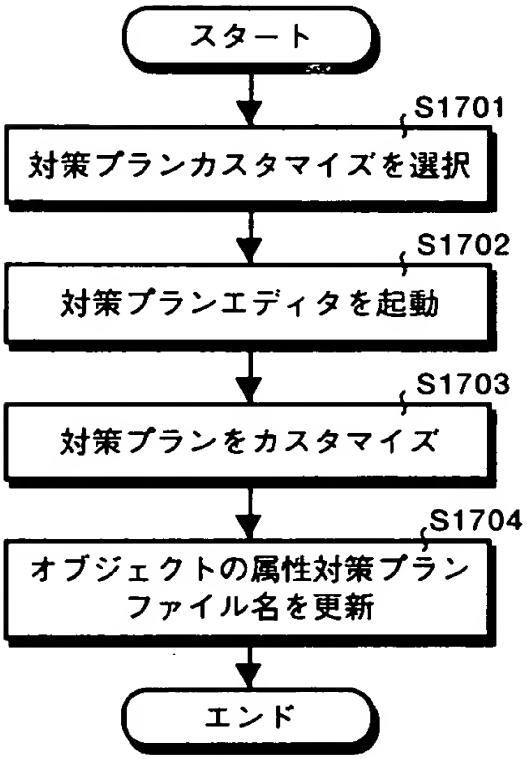
【図１６】

管理マネージャにおける対策ルールの更新手順を説明するための説明図



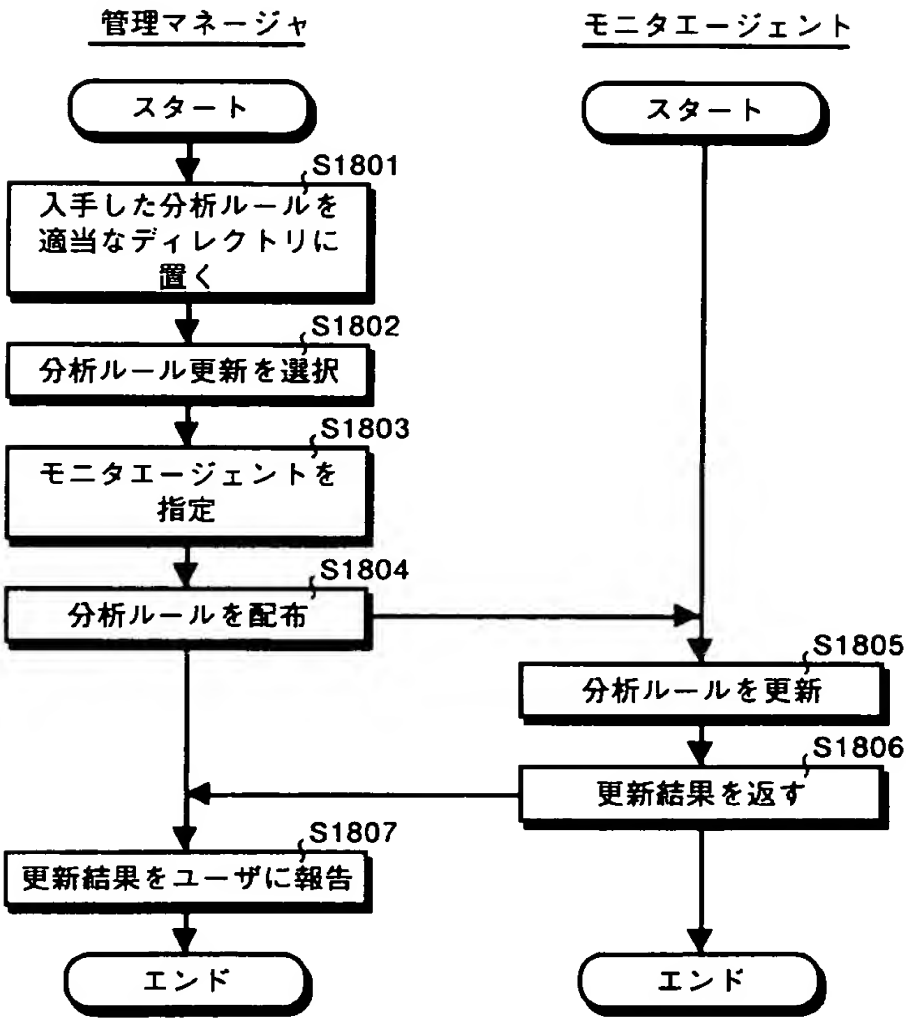
【図１７】

管理マネージャにおいて対策プランをカスタマイズする際の処理手順を示すフローチャート



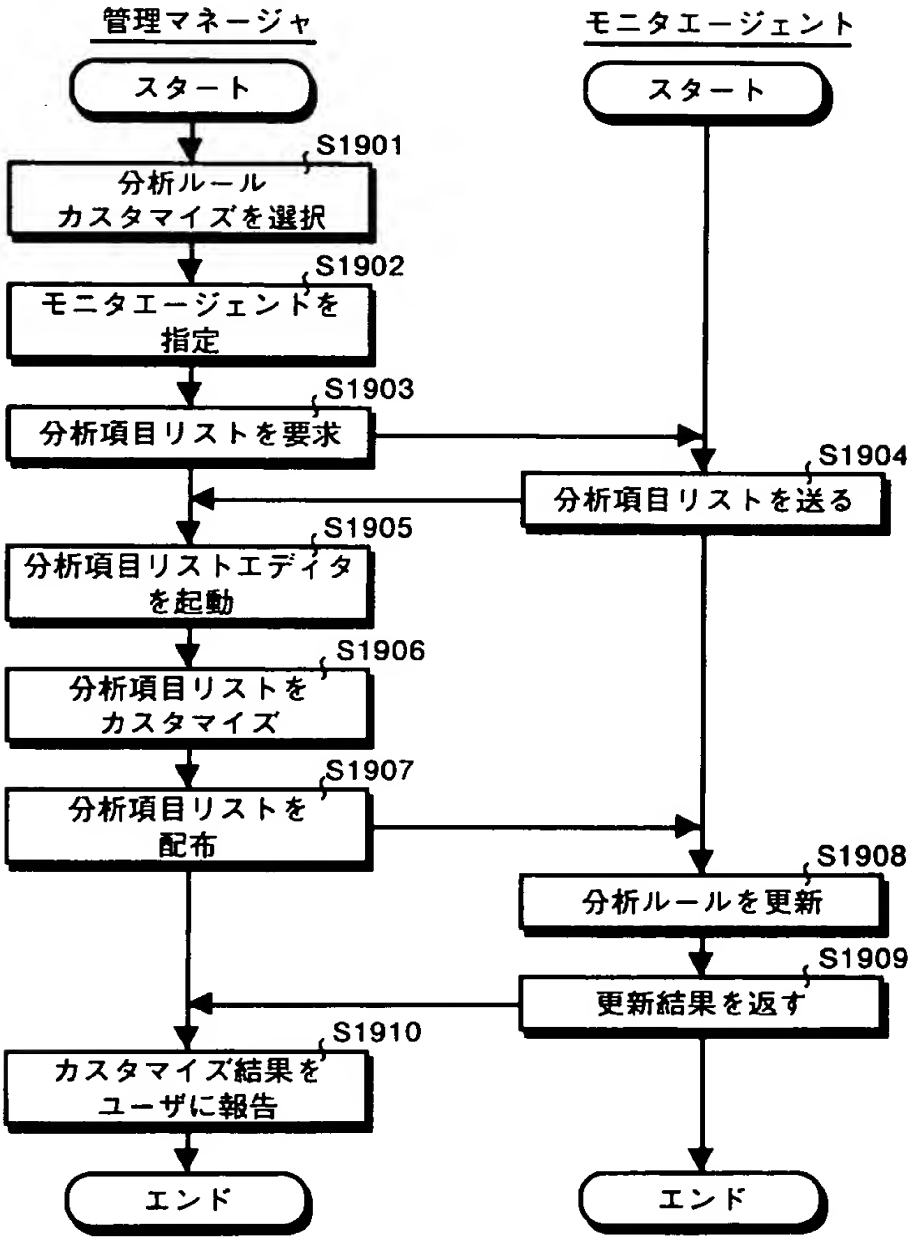
【図１８】

分析ルールを更新する際の管理マネージャとモニタエージェントの処理手順を示すフローチャート



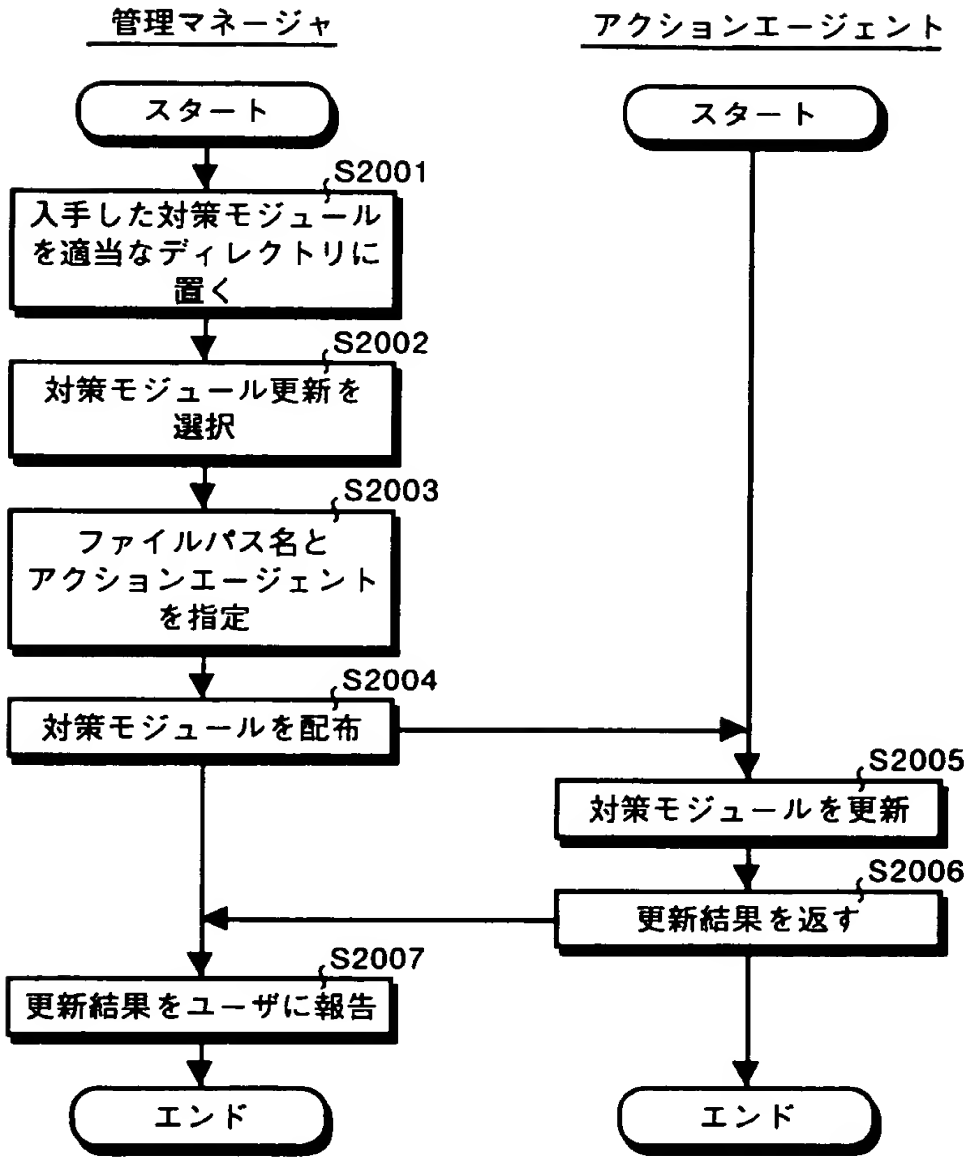
【図１９】

分析ルールをカスタマイズする際の管理マネージャとモニタエージェントの処理手順を示すフローチャート



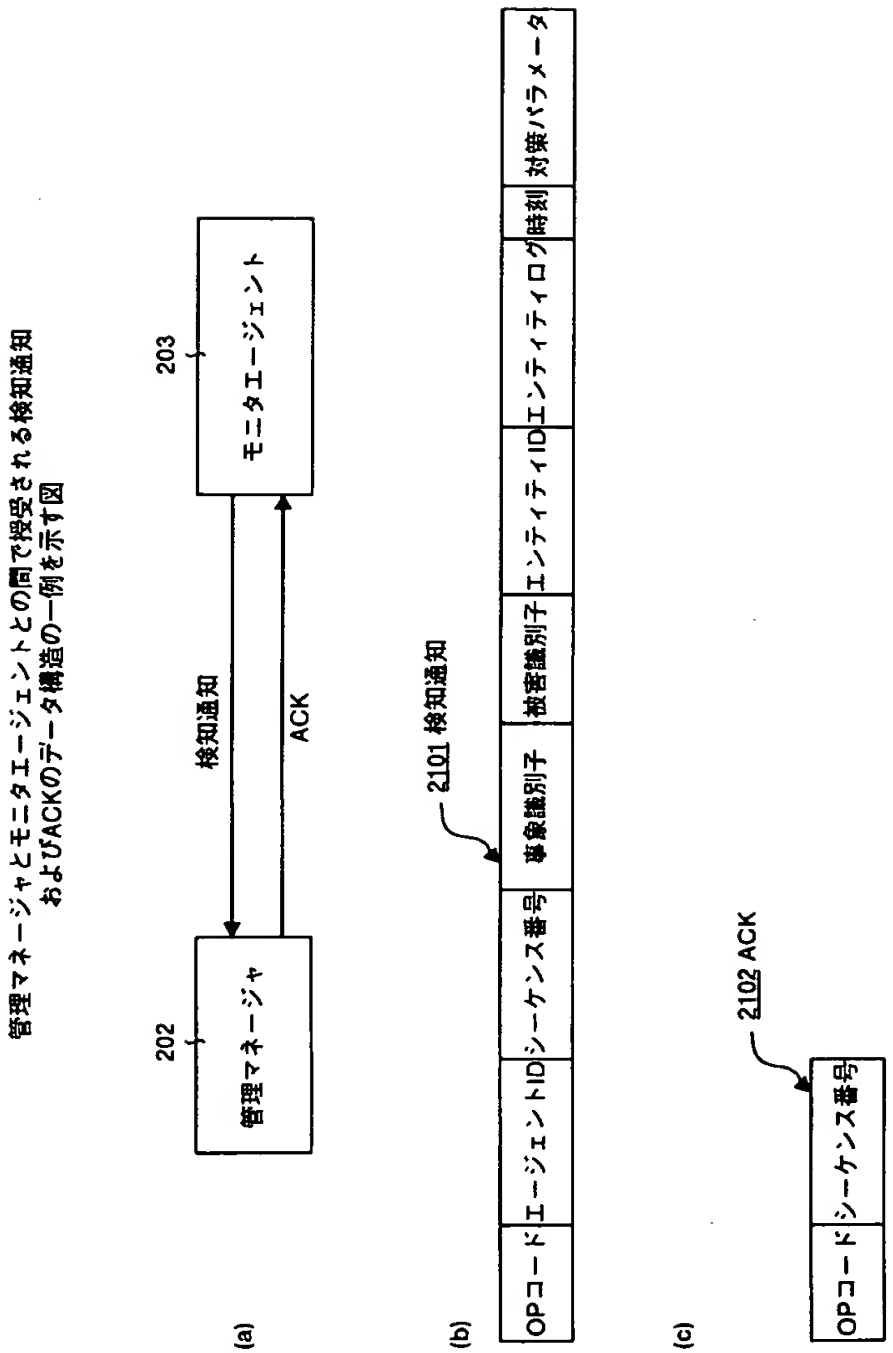
【図２０】

対策モジュールの更新手順を示すフローチャート



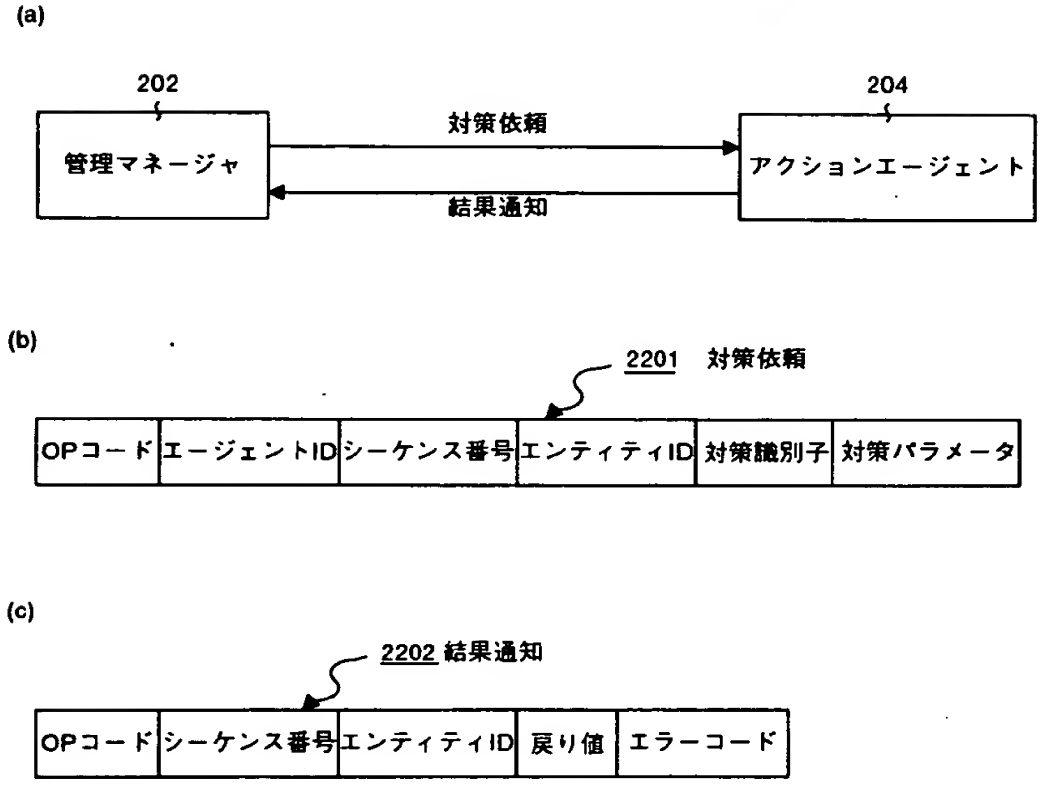
【図２１】

管理マネージャとモニタエージェントとの間で授受される検知通知およびACKのデータ構造の一例を示す図



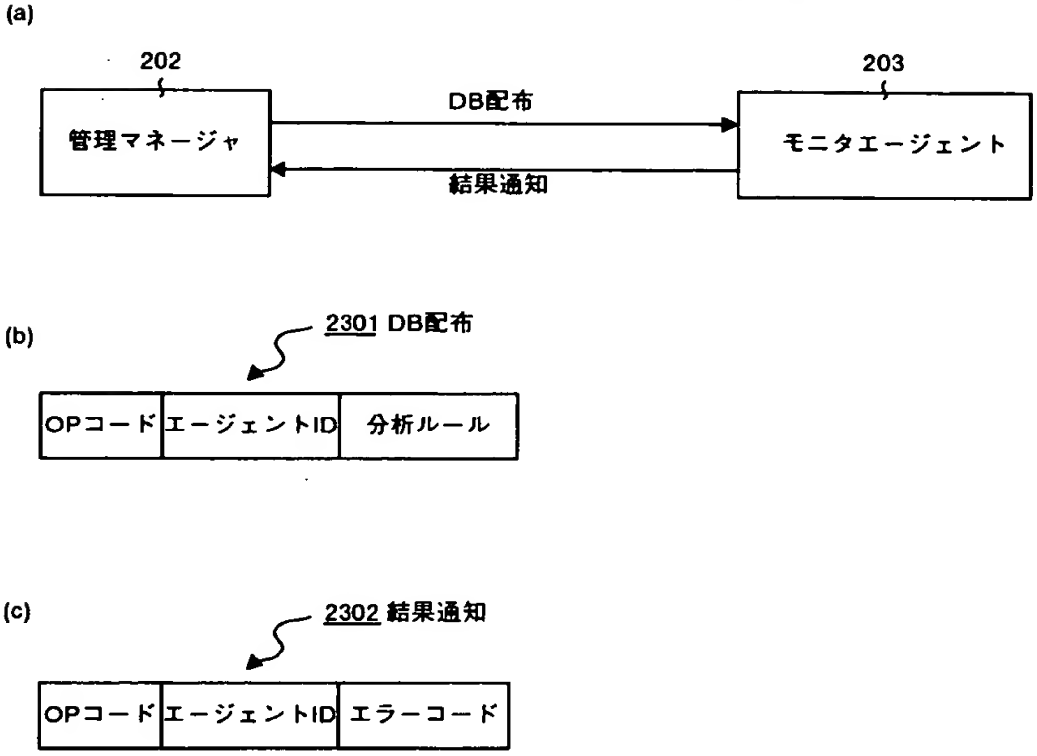
【図２２】

管理マネージャとアクションエージェントとの間で授受される対策依頼
および結果通知のデータ構造の一例を示す図



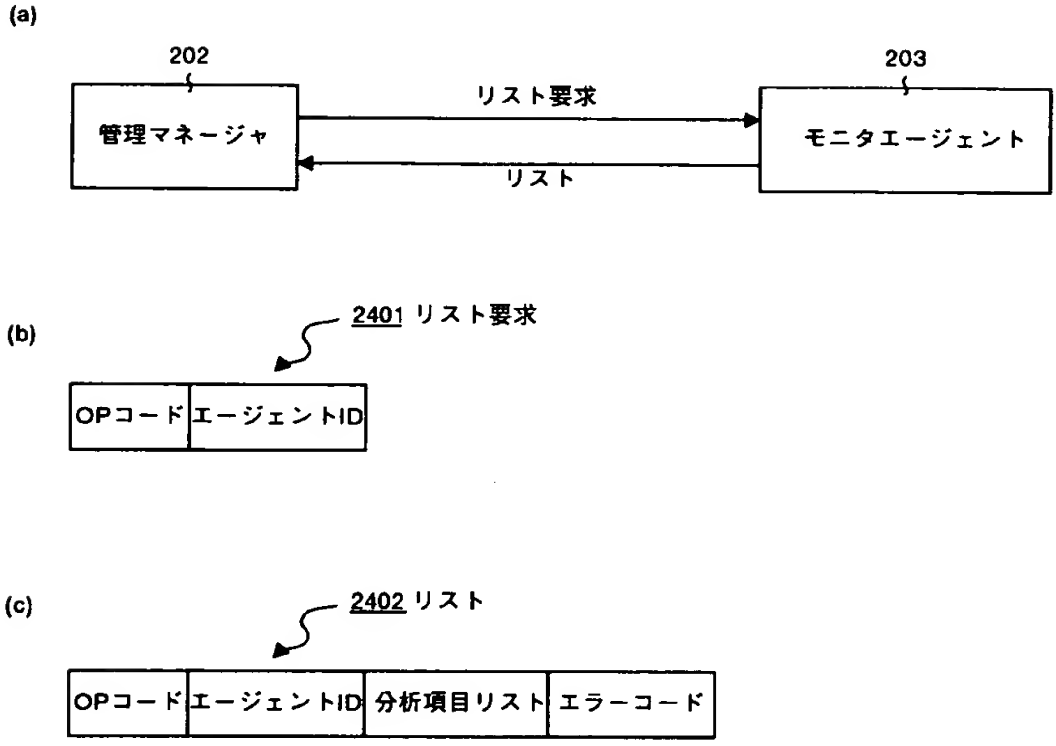
【図２３】

管理マネージャとモニタエージェントとの間で授受されるDB（分析ルール）配布
および結果通知のデータ構造の一例を示す図



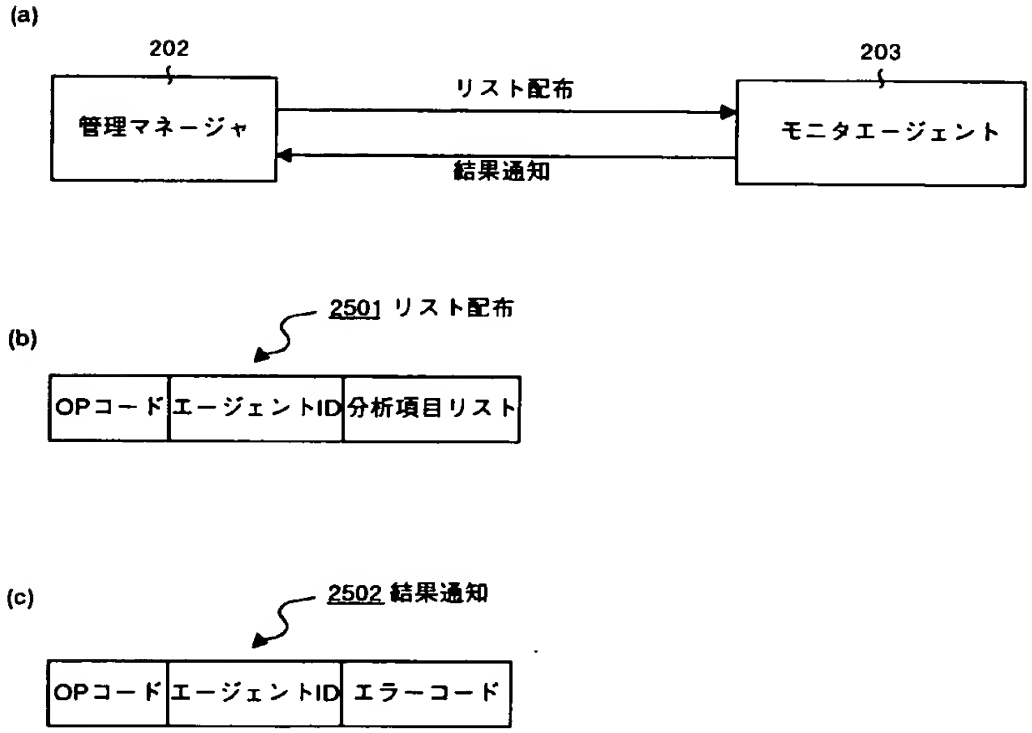
【図２４】

管理マネージャとモニタエージェントとの間で授受されるリスト要求
およびリストのデータ構造の一例を示す図



【図２５】

管理マネージャとモニタエージェントとの間で授受されるリスト配布
および結果通知のデータ構造の一例を示す図

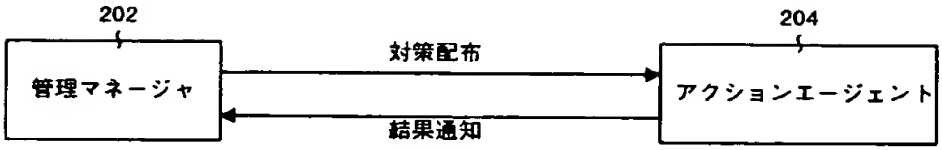


出証特２００１－３０５２４９３

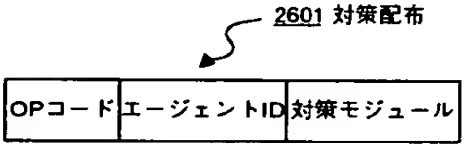
【図２６】

管理マネージャとアクションエージェントとの間で授受される対策配布
および結果通知のデータ構造の一例を示す図

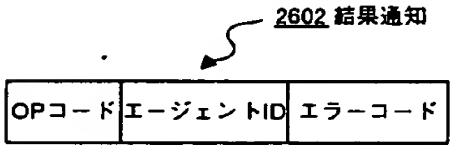
(a)



(b)

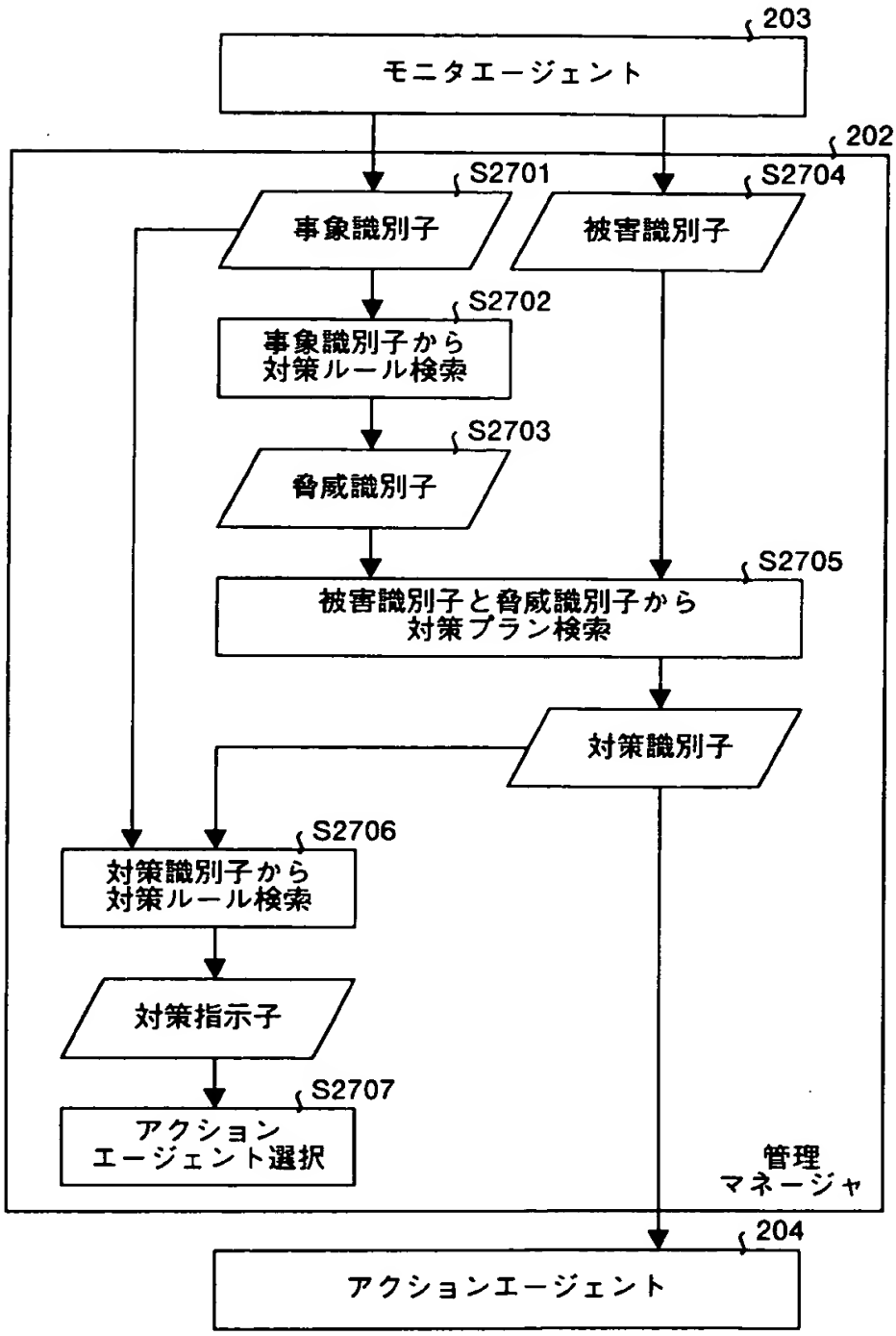


(c)



【図２７】

管理マネージャがおこなう対策決定処理を説明するための説明図



【図２８】

対策プランの一例を示す図

(a)

事象識別子	被害識別子
事象001	被害あり

(b) 対策ルール

事象識別子	脅威識別子	対策識別子	対策指示子
事象001	脅威001	対策001	SERVER
事象001	脅威001	対策002	FW
事象002	脅威001	対策001	SERVER
事象002	脅威001	対策002	FW
事象003	脅威010	対策011	SERVER
事象003	脅威010	対策012	SERVER
事象003	脅威010	対策012	FW
・・・	・・・	・・・	・・・

(c) 対策プラン

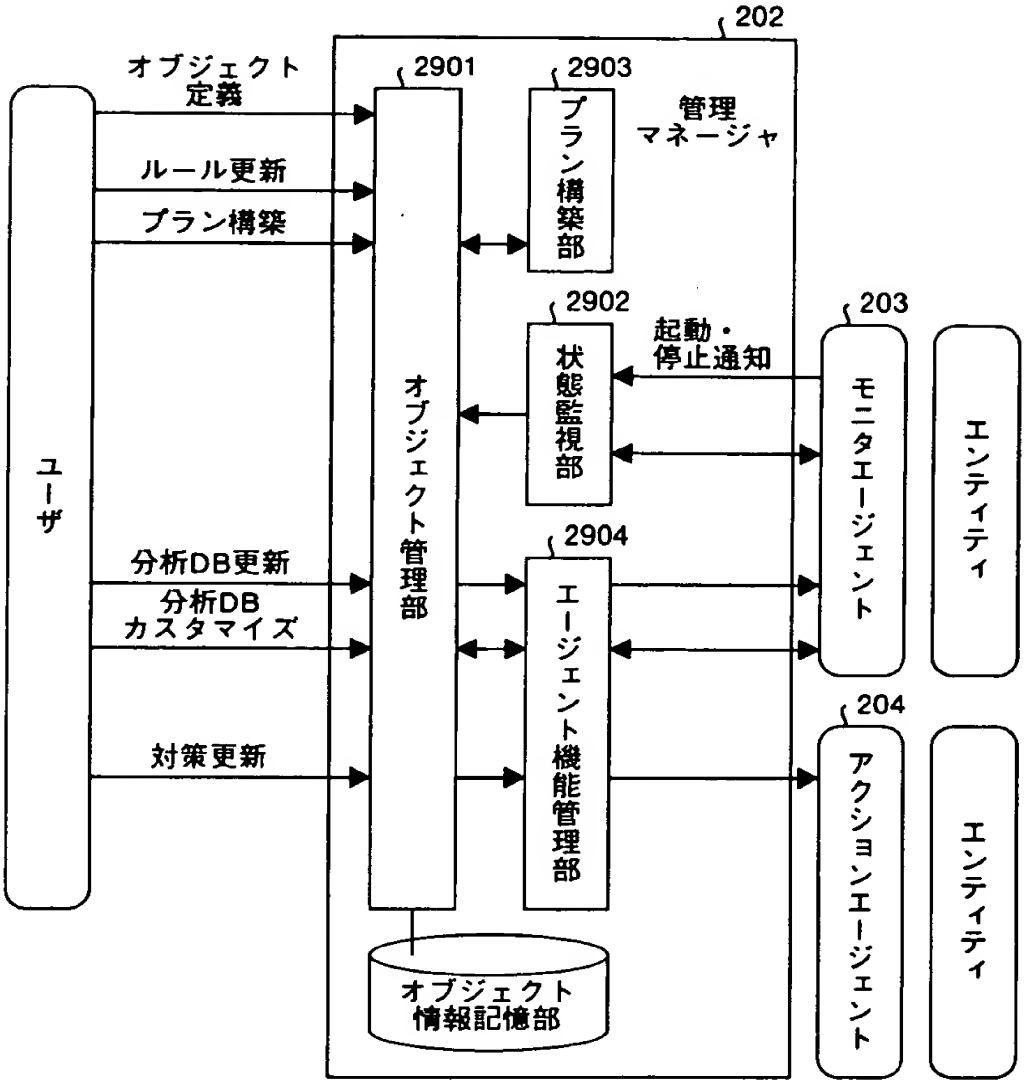
事象識別子	脅威識別子	対策識別子
被害あり	脅威001	対策001
被害不明	脅威001	対策002
被害なし	脅威001	―
被害あり	脅威002	対策011
被害不明	脅威002	―
被害なし	脅威002	―
・・・	・・・	・・・

(d) 対策ルール

事象識別子	脅威識別子	対策識別子	対策指示子
事象001	脅威001	対策001	SERVER
事象001	脅威001	対策002	FW
事象002	脅威001	対策001	SERVER
事象002	脅威001	対策002	FW
事象003	脅威010	対策011	SERVER
事象003	脅威010	対策012	SERVER
事象003	脅威010	対策012	FW
・・・	・・・	・・・	・・・

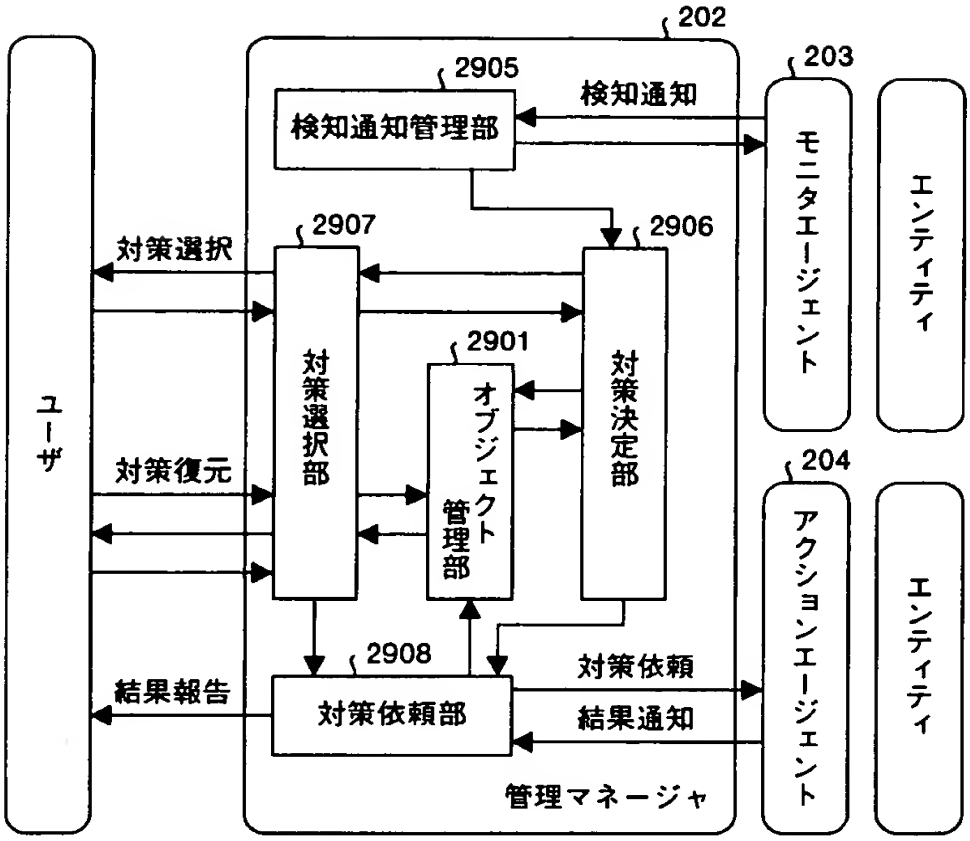
【図２９】

管理マネージャの機能的な構成を示すブロック図



【図３０】

管理マネージャの機能的な構成を示すブロック図



【図３１】

管理マネージャオブジェクトを示す図

属性		説明
管理マネージャ	ID	オブジェクト定義時に、管理マネージャが割り当てる
	IPアドレス	エージェントから管理マネージャへの通信に必要となる情報。ポート番号は、モニタエージェント用、アクションエージェント用の２つ
	ポート番号（1）	
	ポート番号（2）	
	通信タイムアウト値	
	通信リトライ回数	
対策ルール	ファイル名（複数可）	対策ルールファイルへのパスを指定する
対策プラン	ファイル名	対策プランファイルへのパスを指定する
ログフォーマット定義	ファイル名	管理マネージャは、モニタエージェントから送られるエンティティログから時間を引き出す
エージェント認定リスト	ファイル名	認定機関によって認定されたエージェントのリスト。管理マネージャは、リストにないエージェントからの処理を受け付けない
状態監視	時間間隔	エージェントの状態を確認する間隔を指定する
モニタエージェント	ID（複数可）	モニタエージェントをオブジェクト定義すると、自動的に追加される
アクションエージェント	ID（複数可）	アクションエージェントをオブジェクト定義すると、自動的に追加される

【図３２】

エージェントオブジェクトを示す図

属性		説明
エージェント	ID	オブジェクト定義に、管理マネージャが割り当てる
	ステータス	動作状態を示す
	IPアドレス	管理マネージャからエージェントへの通信に必要となる情報
	ポート番号	
	通信タイムアウト値	
	通信リトライ回数	
エンティティ	ID	エージェントの対象エンティティ
管理マネージャ	ID	エージェントの管理マネージャ

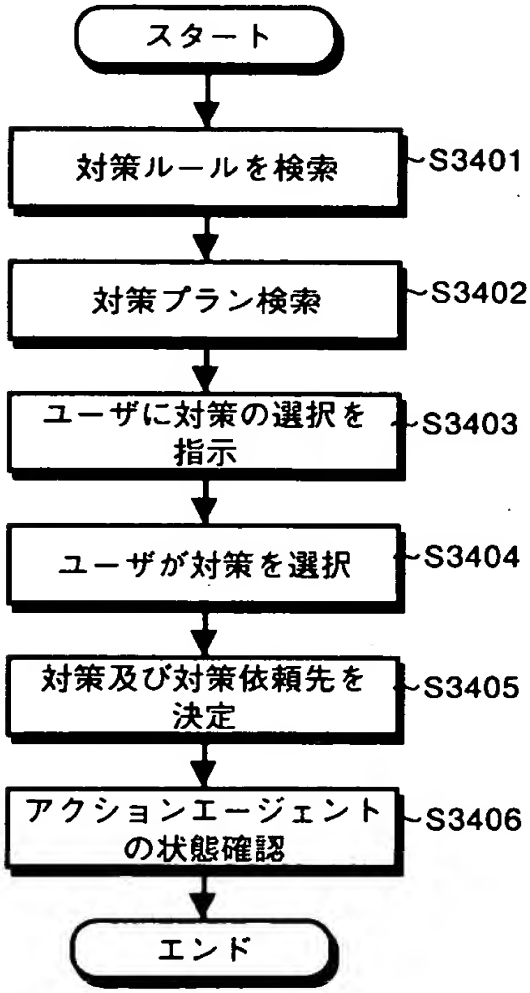
【図３３】

エンティティオブジェクトを示す図

属性		説明
エンティティ	ID	オブジェクト定義時に、管理マネージャが割り当てる
	IPアドレス	エージェントからエンティティへの通信に必要となる情報
	ポート番号	
	通信タイムアウト値	
	通信リトライ回数	
FW エンティティ	ID	エンティティのファイアウォールにあたるエンティティ
モニタ エージェント	ID	モニタエージェントをオブジェクト定義すると、自動的に追加される
アクション エージェント	ID	アクションエージェントをオブジェクト定義すると、自動的に追加される
対策履歴	（複数可）	対策依頼、もしくは対策結果を履歴として残す
エンティティ固有情報	FireWall-1	FireWall-1オブジェクト名

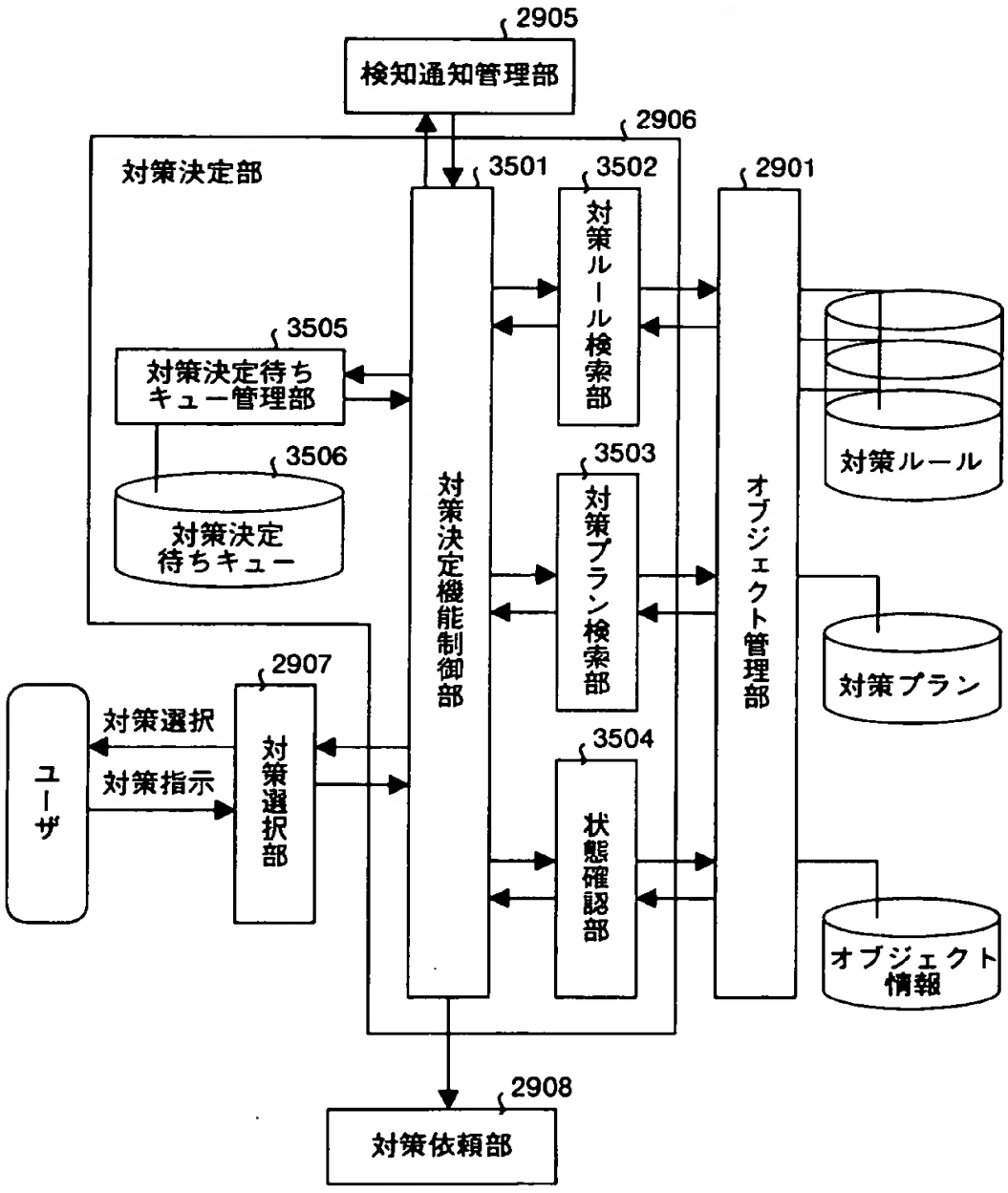
【図３４】

対策決定部による対策決定までの処理手順を示すフローチャート



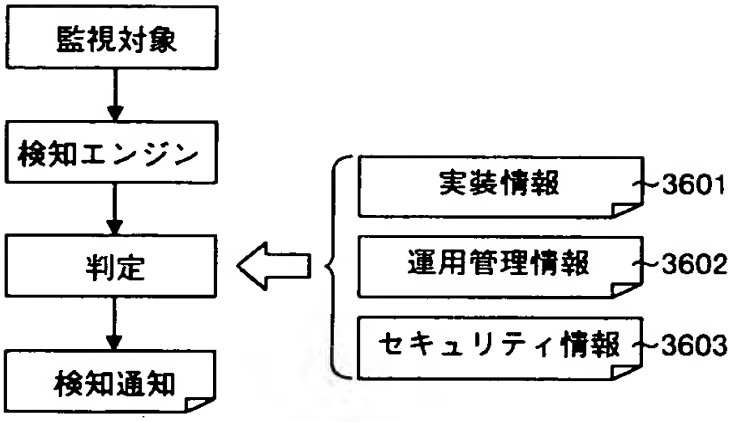
【図３５】

対策決定部の構成を示す機能ブロック図



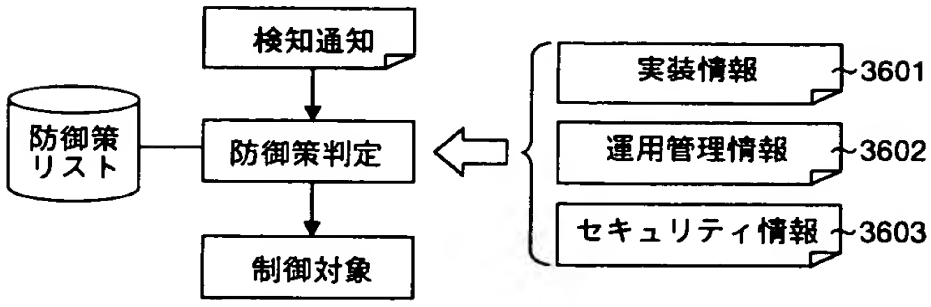
【図３６】

レポーティング機能を説明するための説明図



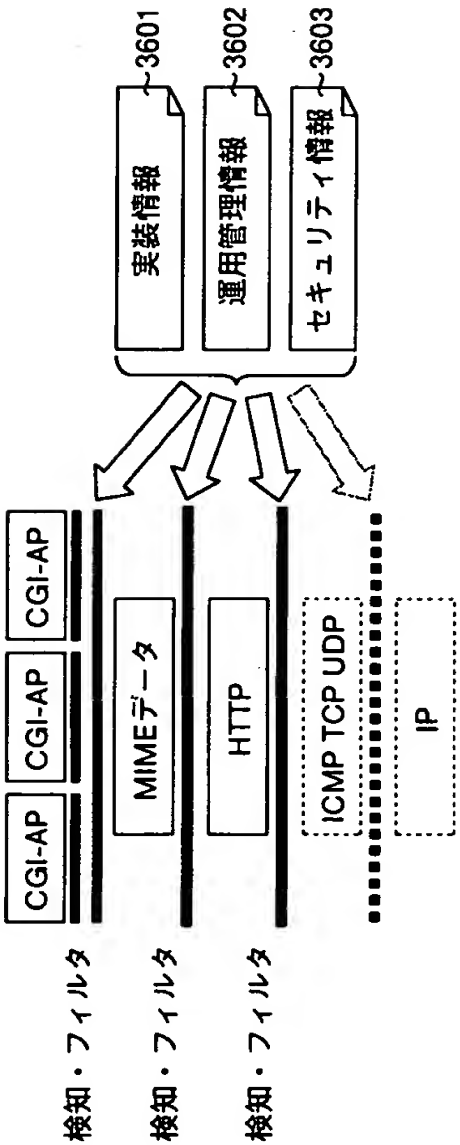
【図３７】

実装情報などを用いた多面的な防御策選択を
説明するための説明図



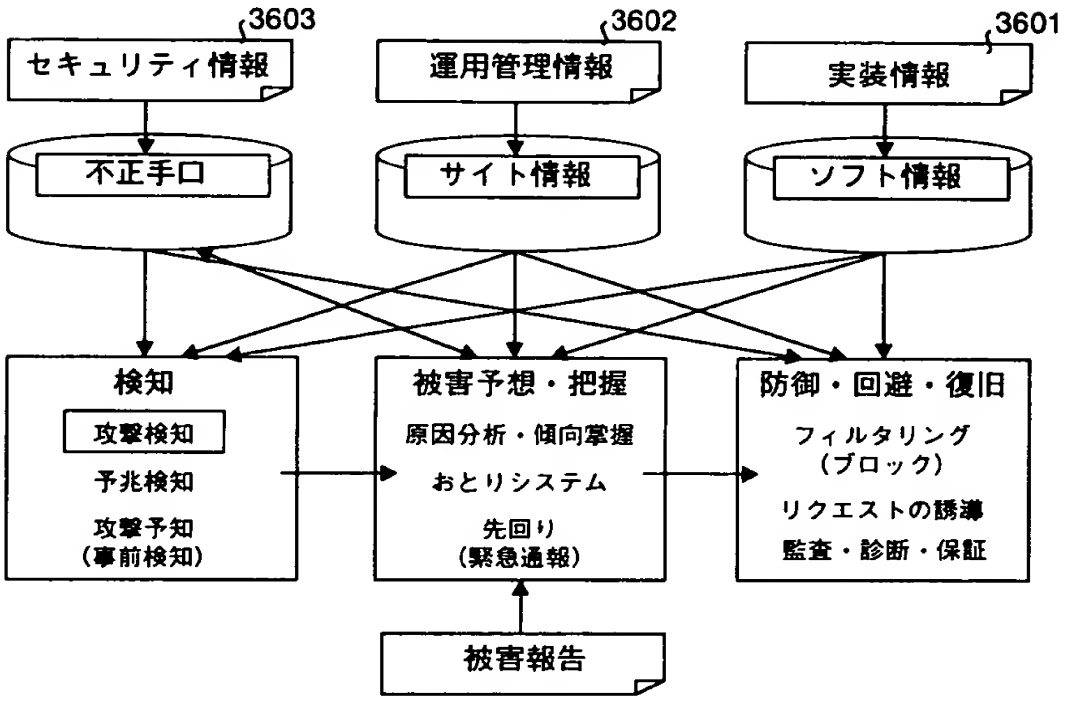
【図３８】

実装情報などをプロトコル階層間のフィルタとして用いる概念を説明するための説明図



【図３９】

実装情報、運用管理情報およびセキュリティ情報を用いた統合連携制御を説明するための説明図



【書類名】　　要約書

【要約】

【課題】　サイトに対する攻撃の予兆を検知して、実際の攻撃が開始される前に対策を施し、もって被害の極小化を図ることを課題とする。

【解決手段】　モニタエージェント２０３でエンティティのログを分析し、異常の予兆を検知した場合には、管理マネージャ２０２に通知する。そして、この管理マネージャ２０２は、データベース２０１などに基づいて対策および対策依頼先を決定し、対策依頼先であるアクションエージェント２０４に該当する対策を実施させる。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社